LevelOne

User Manual

WBR-6603

150Mbps Wireless ADSL2+ Modem Router

Ver. 1.0

Safety

FCC WARNING

This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1) Reorient or relocate the receiving antenna.
2) Increase the separation between the equipment and receiver.
3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4) Consult the dealer or an experienced radio/TV technician for help.

CE Declaration of conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

CE Marking Warning

Hereby, Digital Data Communications, declares that this product (Model-no. WBR-6603) is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The CE-Declaration of Conformity can be downloaded at:

http://www.levelone.eu/support.php

The specification is subject to change without notice.

General Public License

This product incorporates open source code into the software and therefore falls under the guidelines governed by the General Public License (GPL) agreement.

Adhering to the GPL requirements, the open source code and open source license for the source code are available for free download at http://global.level1.com.

If you would like a copy of the GPL or other open source code in this software on a physical CD medium, LevelOne (Digital Data Communications) offers to mail this CD to you upon request, for a price of US$9.99 plus the cost of shipping.

Table of Content

TABLE OF CONTENT **4**

1. INTRODUCTION **5**

USER MANUAL OVERVIEW 5

2. UNPACKING AND SETUP **6**

FEATURES 6

PACKAGE CONTENTS 6

3. HARDWARE INSTALLATION **7**

FRONT VIEW 7

REAR VIEW 8

HARDWARE INSTALLATION STEPS 9

4. CHECK YOUR NETWORK SETTINGS **10**

5. GETTING START **11**

6. ADVANCED SETUP **17**

BASIC SETTING 18

Primary Setup *19*

DHCP Server *27*

Wireless Settings *28*

Change Password *38*

FORWARDING RULES 39

Virtual Server *40*

Special AP *41*

Miscellaneous *42*

Packet Filter *44*

Packet Filter *44*

Domain Filter *49*

URL Blocking *50*

MAC Control *51*

Miscellaneous *53*

System Time *55*

System Log *56*

Dynamic DNS *57*

SNMP Setting *58*

Routing *59*

Schedule Rule *61*

Toolbox *63*

View Log *64*

Firmware Upgrade *65*

Backup Setting *65*

Reset to Default *65*

Reboot *65*

Miscellaneous *66*

TECHNICAL SPECIFICATIONS **76**

Default Settings

IP Address	192.168.1.1
Password	admin
Wireless Mode	Enable
Wireless SSID	LevelOne
Wireless Security	None

1. Introduction

Congratulations on your purchase of LevelOne WBR-6603 *150Mbps Wireless ADSL2+ Modem Router*. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users.

Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read the manual carefully for fully exploiting the functions of this product.

User Manual Overview

Introduction	Describes the *150Mbps Wireless ADSL2+ Modem Router*.
Unpacking and Setup	Helps user to get started with the basic installation of the *150Mbps Wireless ADSL2+ Modem Router*.
Hardware Installation	Describes the LED indicators of the *150Mbps Wireless ADSL2+ Modem Router*.
Configuration	Describes the functionalities and its settings.
Technical Specifications	Lists the technical (general, physical and environmental) specifications of the *150Mbps Wireless ADSL2+ Modem Router*.

2. Unpacking and Setup

This chapter provides the package contents and setup information for the *150Mbps Wireless ADSL2+ Modem Router*.

Features

- Integrates 4-Port 10/100Mbps Fast Ethernet Switch with Auto-MDI/MDIX
- Compatible with IEEE 802.11n standard and up to 150Mbps data rates
- Allows several users to access Internet through Network Address Translation (NAT, IP sharing)
- simultaneously
- Supports wireless signal On / Off button
- Simple Wireless Security with one-push WPS button
- Supports Internet access control (URL Blocking, MAC Filtering)
- Supports multiple sessions IPSec, L2TP and PPTP VPN pass-through
- Supports QoS for traffic prioritization

Package Contents

Open the box of the *150Mbps Wireless ADSL2+ Modem Router* and carefully unpack it. The box should contain the following items:

-WBR-6603

-Power Adapter

-RJ-11 ADSL/ Telephone Cable

-RJ-45 LAN Ethernet Cable

-CD Manual/QIG

-Quick Installation Guide

If any item is found missing or damaged, please contact your local reseller for replacement.

3. Hardware Installation

Front View

1) Status

- A steady blinking light indicates the device is ready

2) ADSL

- A solid light indicates the ADSL port is connected.

3) WLAN

- A solid light indicates the Wireless LAN is turned on and ready for use.
- Off indicates Wireless LAN is turned off.
- LED blinks during wireless data transmission.
- Steady blinking indicates WPS function is activated and the router is pairing with wireless client.

4) LAN Lights

- A solid light indicates to an Ethernet enable computer on ports 1 ~ 4.
- LED blinks during data transmission.

5) Wireless On/Off Button

- Press and hold for 3 seconds to turn the Wireless LAN on or off.
- Please confirm WLAN status as indicated by WLAN Light

5) WPS Button

- It is Wi-Fi Protected Setup push button. Press and hold for 5 seconds to activate WPS pairing with wireless client when WLAN is on.

Note: You can reset the device by pressing “Wireless on/off” and “WPS” button for 5 seconds simultaneously.

Rear View

1) Antenna

- 2dBi fix antenna.

2) LAN Ports (1~4)

- Connect Ethernet devices such as computers, switches or hubs.

3) DSL Port

- The DSL port is the connection for the RJ-11 telephone cable to the ADSL terminator connection.

4) Power Jack

- Receptor for the supplied power adapter

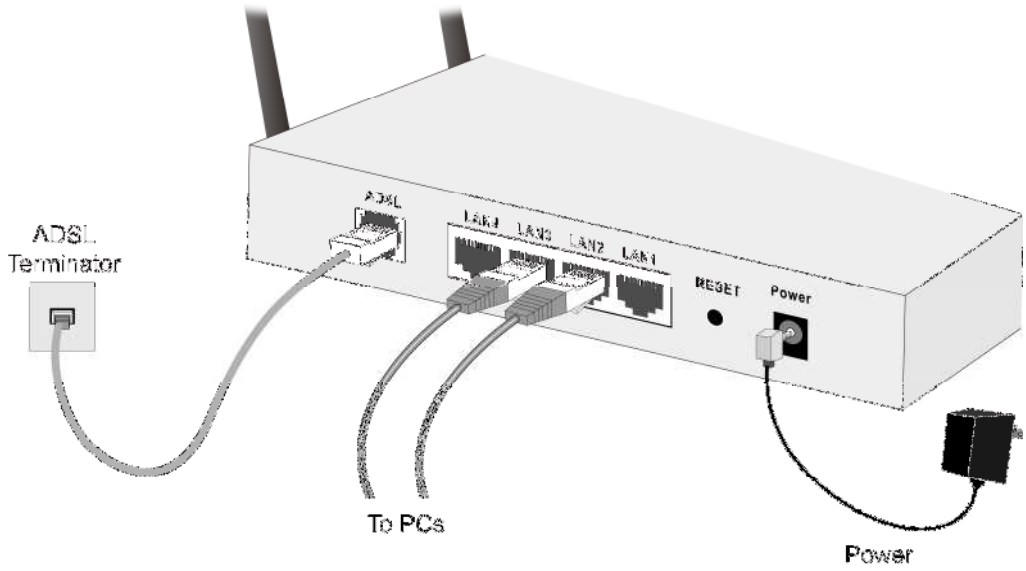
Hardware installation steps

Decide where to place your Wireless ADSL Router

You can place your Wireless ADSL Router on a desk or other flat surface. For optimal performance, place your Wireless ADSL Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

Setup LAN connection

- Wired LAN connection: Connect an Ethernet cable from your computer's Ethernet port to one of the LAN ports of the Wireless Router.
- Wireless LAN connection: Locate the WBR-6603 at a proper position to gain the best transmit performance.



3. Setup ADSL connection

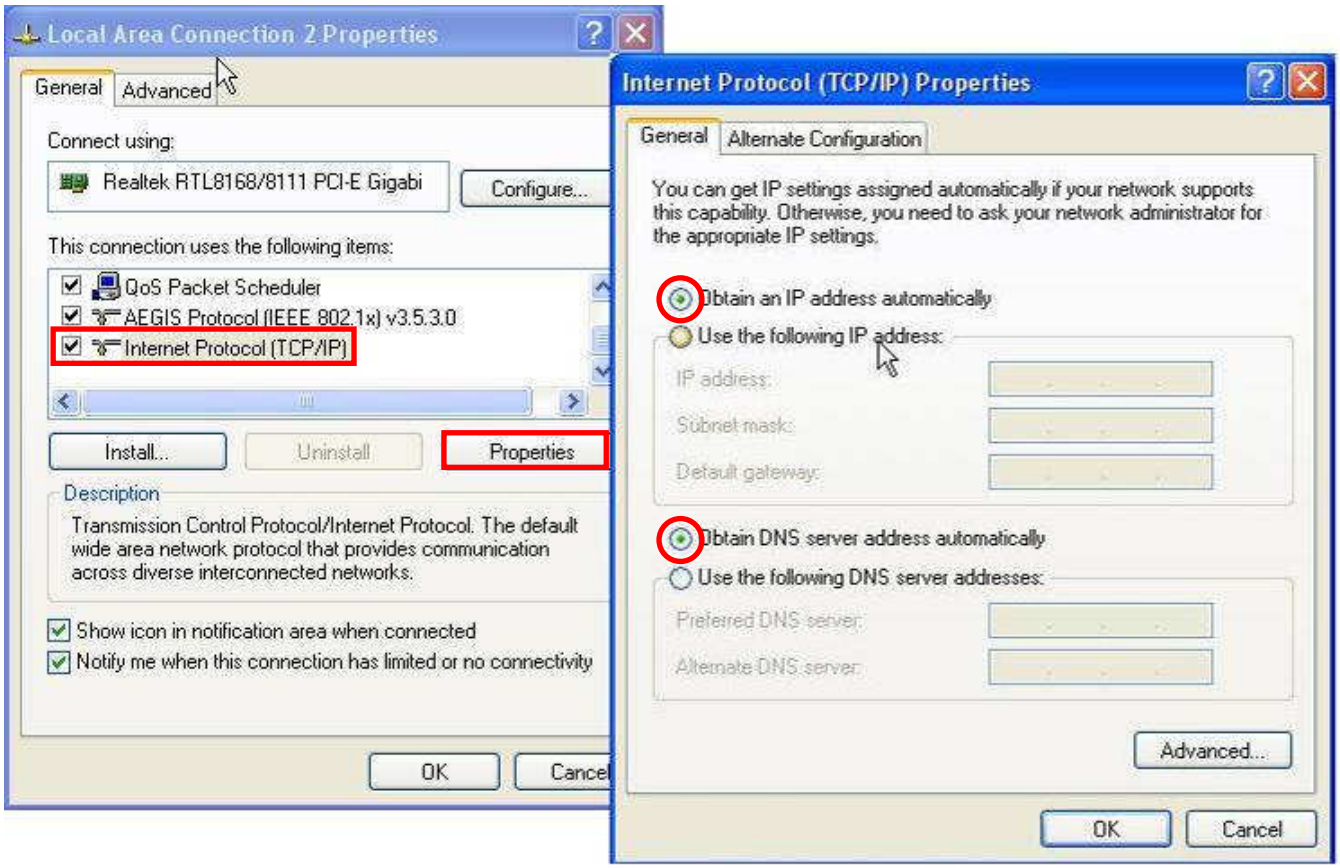
Connect the supplied ADSL cable from to the ADSL port on the Wireless ADSL Router (the DSL RJ11 connector) to the ADSL terminator provided by your phone company.

4. Power on

Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the **Status** indicator will be lighted ON, and the Status indicator will be continuously flashing once per second to indicate that this product is in normal operation.

4. Check Your Network Settings

1. Please make sure your PC can get IP address automatically so the WBR-6603 can communicate with your PC during configuration.
   - Select “Control Panel” > “Network Connections”.
   - Right click the “Local Area Connection” and choose “Properties”.
   - Select the TCP/IP protocol for your network card.
   - Click on the Properties button. You should then see the following screen and make sure you have selected “Obtain IP address automatically”


Local Area Connection 2 Properties
General
Advanced
Connect using:
Realtek RTL8168/8111 PCI-E Gigabi
Configure...
This connection uses the following items:
QoS Packet Scheduler
AEGIS Protocol (IEEE 802.1x) v3.5.3.0
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2. Reboot computer to make sure you have received the IP address correctly.

5. Getting Start

Configuration Wizard

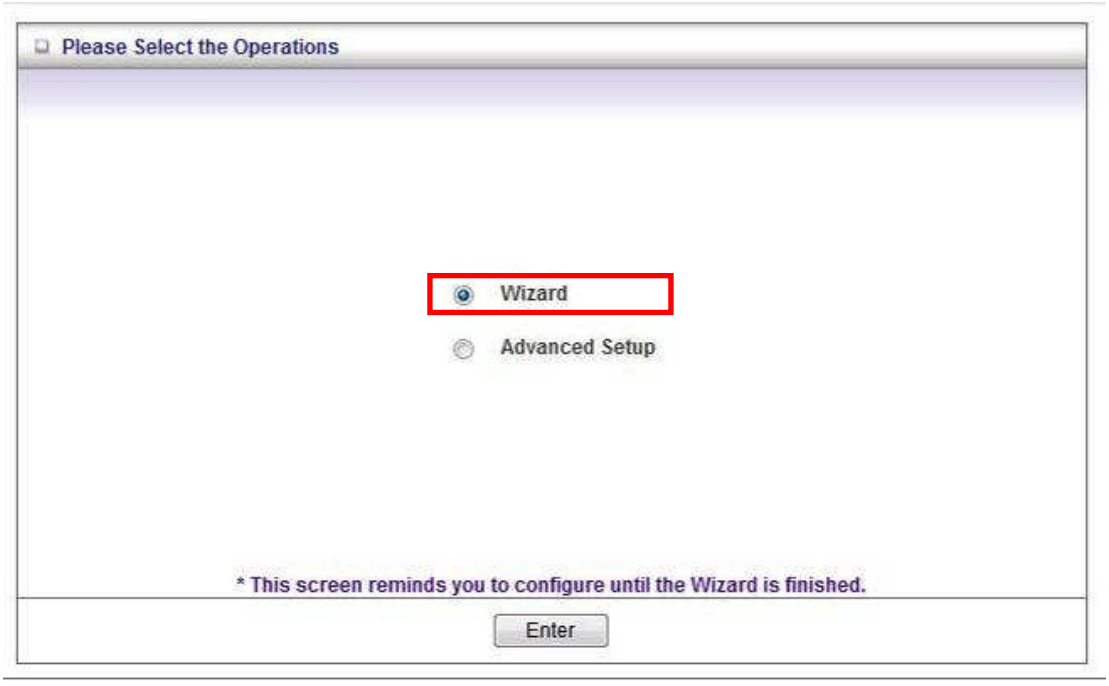
Once properly configured, the WBR-6603 *150Mbps Wireless ADSL2+ Modem Router* will obtain and assign IP address information automatically. Configuration settings can be established through the Web-Based Configuration Menu.

Open a web browser (Internet Explorer/Firefox/Safari) and type in the IP Address http://192.168.1.1

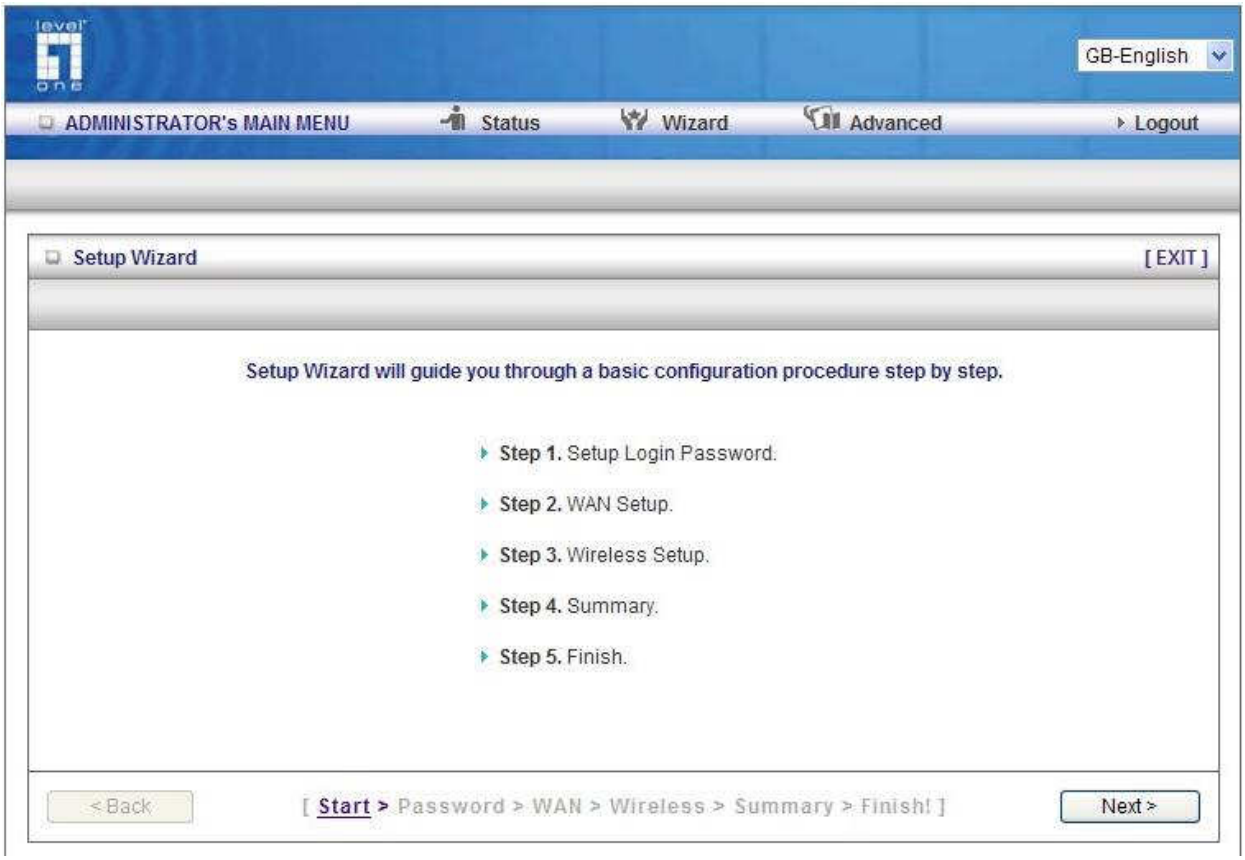
Note:
If you have changed the default IP Address assigned to the WBR-6603, ensure you enter the correct IP Address.

Type in "**admin**" (without quotes) in the Password box, then click Login.
Note: admin is the default login password for the unit.

The user can setup step by step to finish the connection with Wizard.
If you are an advanced user, you can access the configurations directly in the Advanced Setup


Please Select the Operations
Wizard
Advanced Setup
* This screen reminds you to configure until the Wizard is finished.
Enter

Setup Wizard will guide you through a basic configuration procedure step by step. Press **Next** to begin.



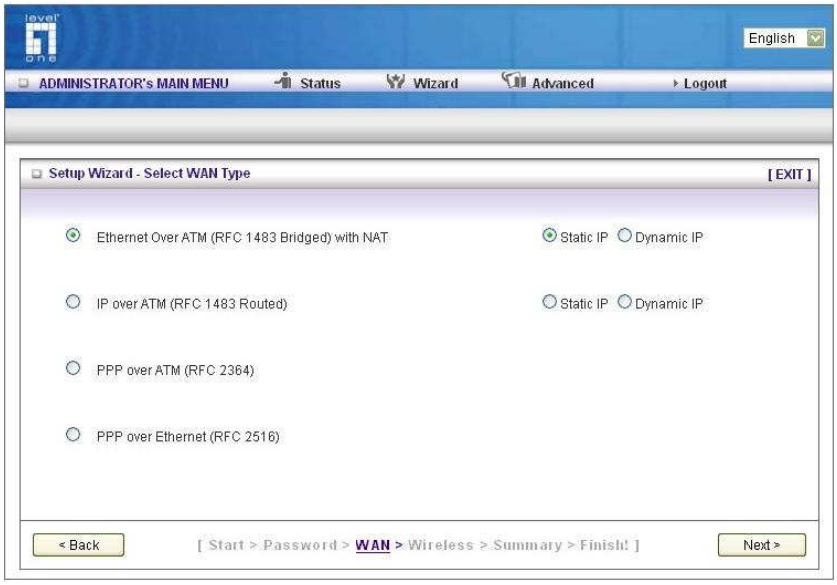
Step 1:

You can change system password in this page, set up your system password.

Press “Next”

Step 2:

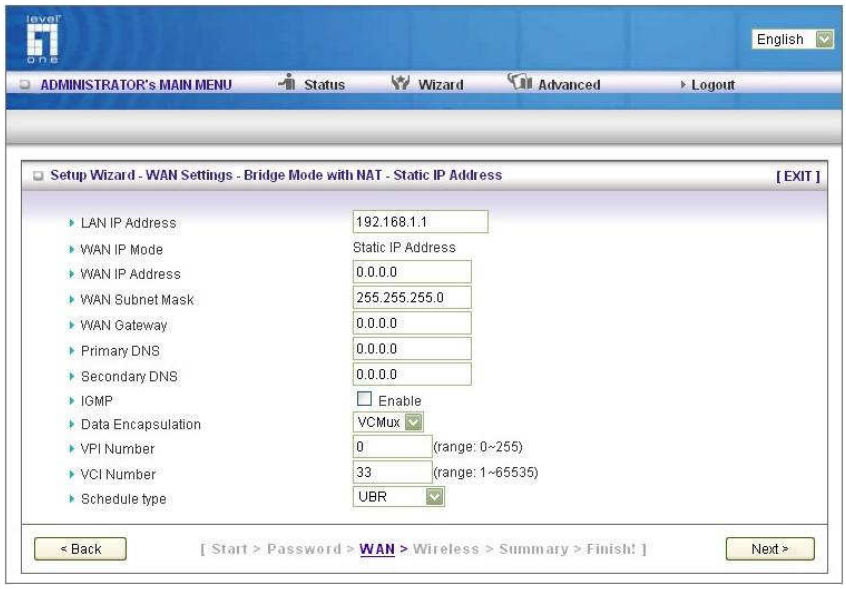
Setup WAN Type of your internet, then press “Next”



Step 3:

If you choose WAN type of Bridge mode with NAT-Dynamic IP address, Setup the LAN IP, Host Name information, and WAN Mac address, then press “Next”

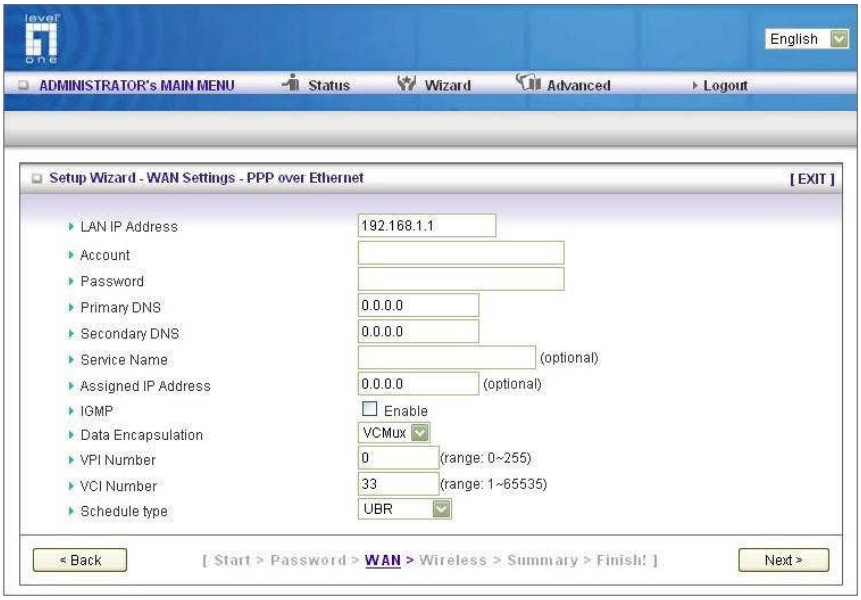
If you choose WAN type of Bridge mode with NAT-Static IP address, setup the LAN IP, WAN IP, Gateway, Subnet Mask and DNS information, then press “Next”



Step 4:

If you choose WAN type of PPP over Ethernet, please fill in PPPoE service information which is provided by your ISP.

After setup, press “Next”



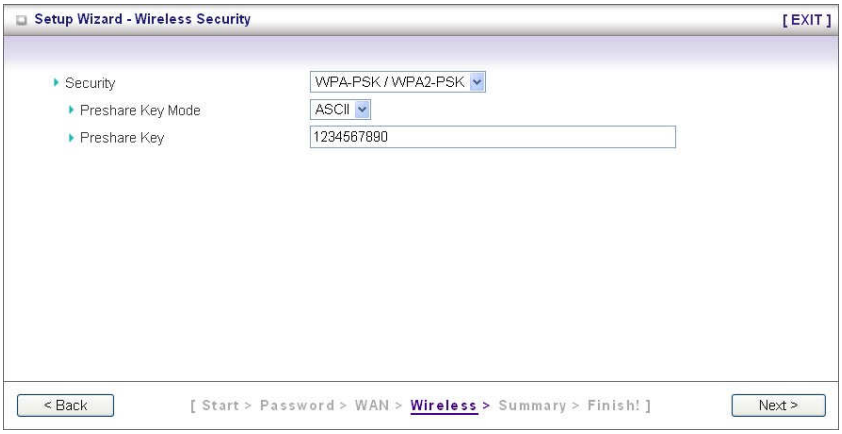
Step 5:

Set up your Wireless settings, you can Enable/Disable wireless, setup, setup your Network SSID information, and configure wireless channel in this page.

After setup, press “Next”

Set up your wireless security encryption. It is suggest to use WPA-PSK/WPA2-PSK to have stronger wireless encryption.

After setup, press “Next”

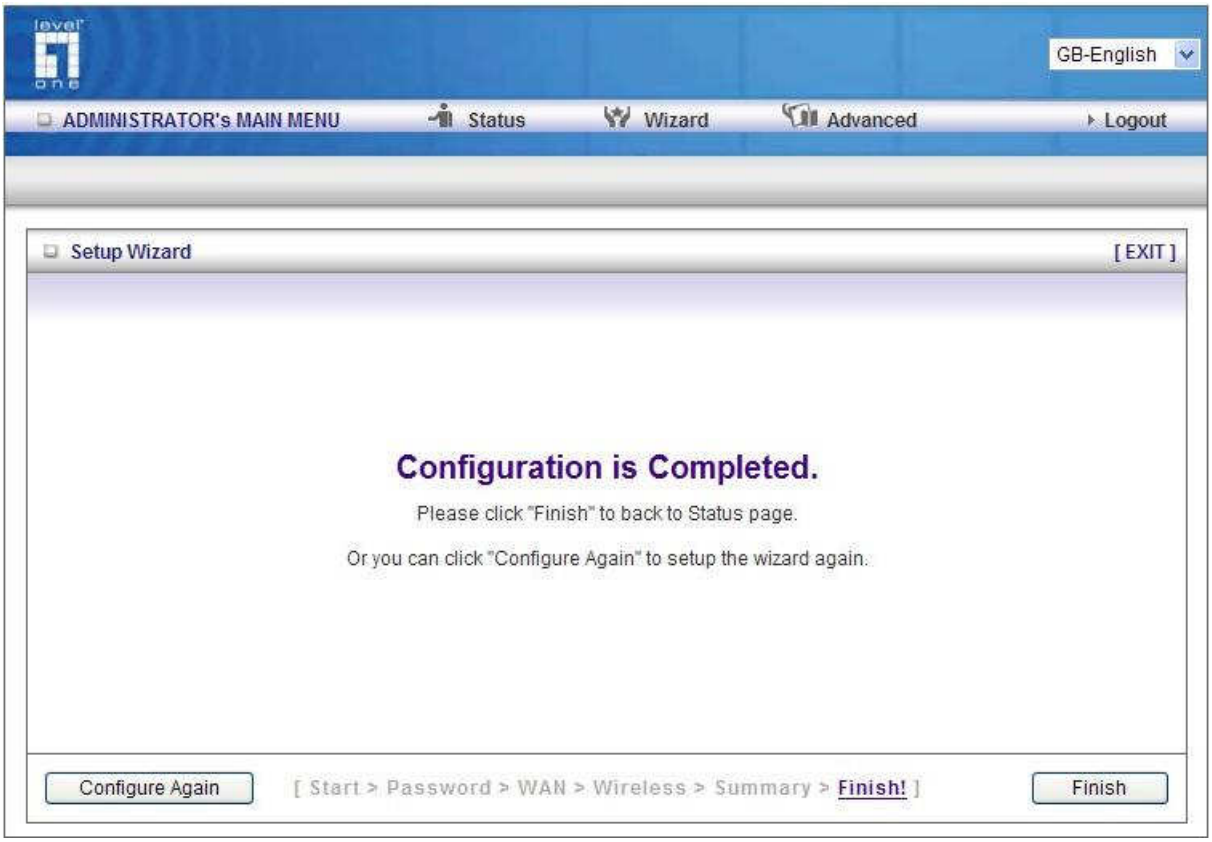


Step 6:

Check all settings is correct, then click “Apply Setting” button.

The device will automatically reboot to make the settings effect.

Once the user finishes those steps and the router screen displayed as below. It means that the Internet connection is now established.



System Status

This option provides the function for observing this product's working status:

WAN Port Status:

If the WAN port is assigned a dynamic IP, there may appear a "**Renew**" or "**Release**" button on the sidenote column. You can click this button to renew or release IP manually.

Wireless Status:

You can check your Wireless settings in this column.

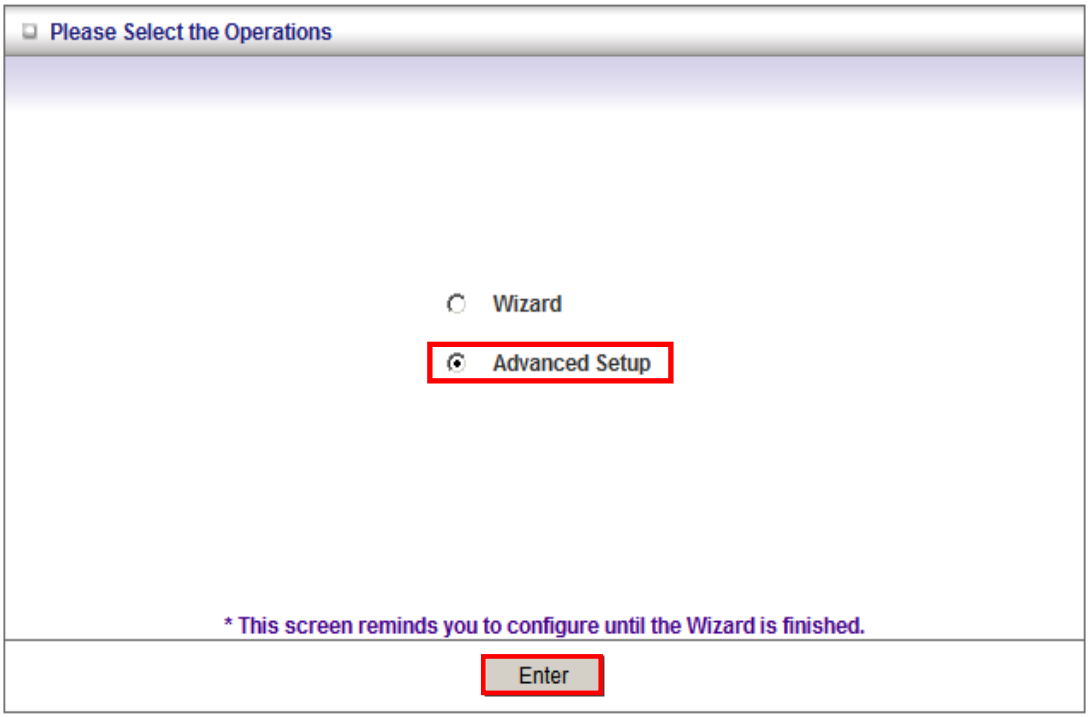
Statistics of WAN:

Enables you to monitor inbound and outbound packets

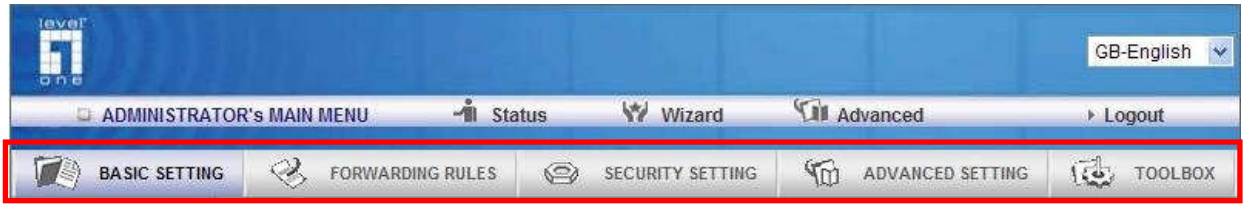
6. Advanced Setup

To access the Advanced Setup, click on **Advanced Setup** at the top of the page.

Or, for first time installation, choose Advanced Setup and click **Enter**.

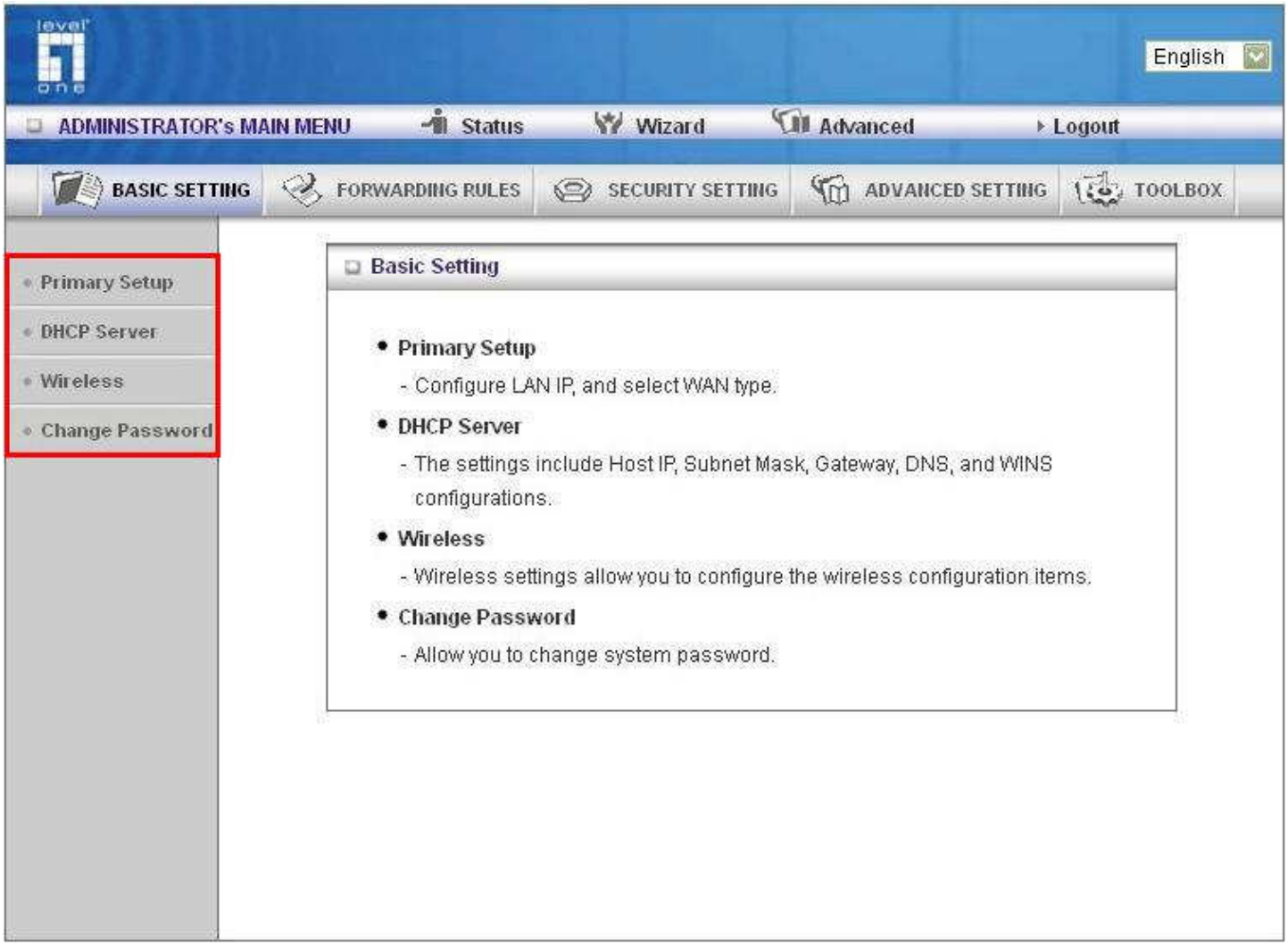

Please Select the Operations
Wizard
Advanced Setup
* This screen reminds you to configure until the Wizard is finished.
Enter

Once in the Advanced Setup, you will be presented with the following menu.



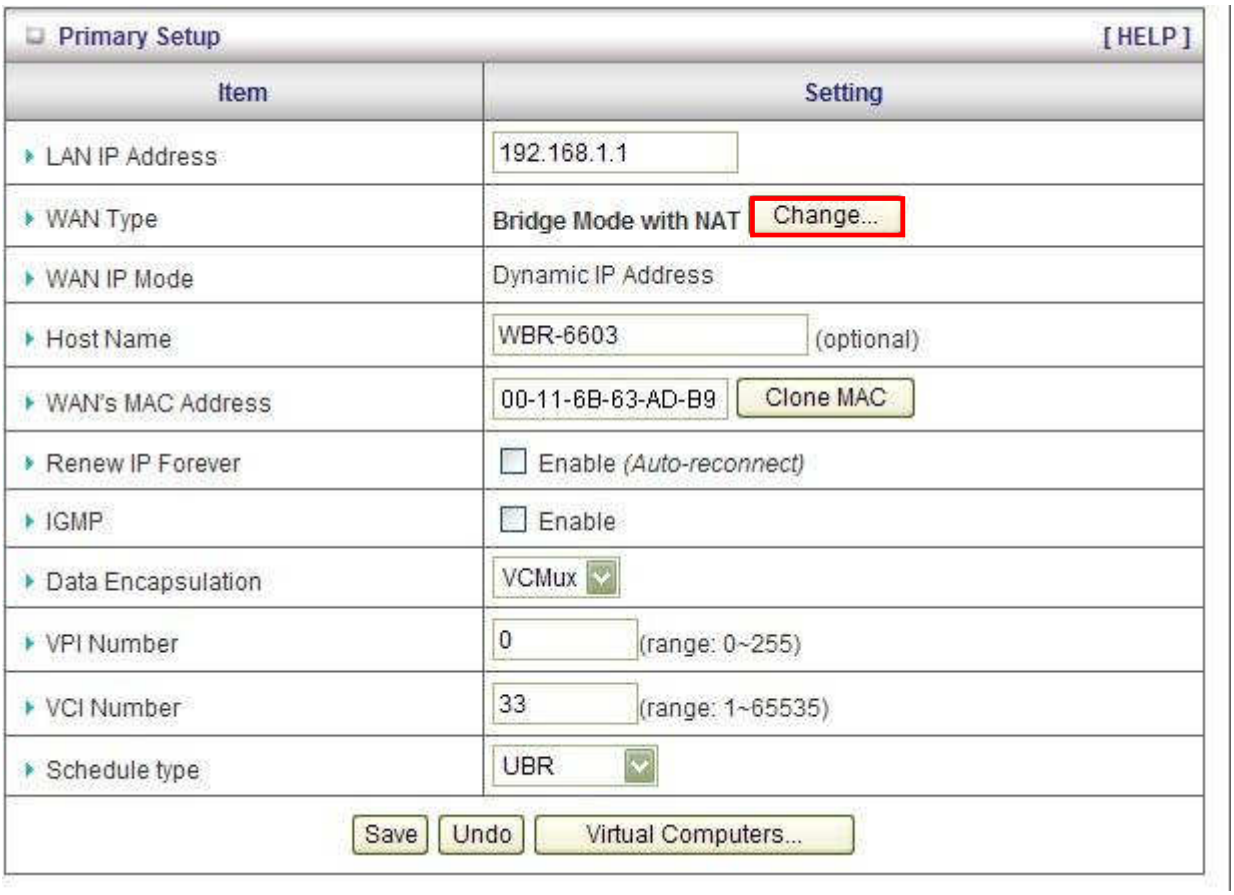
Basic Setting

These are the basic settings of the unit. Click on the menu on the left to access the respective settings page.



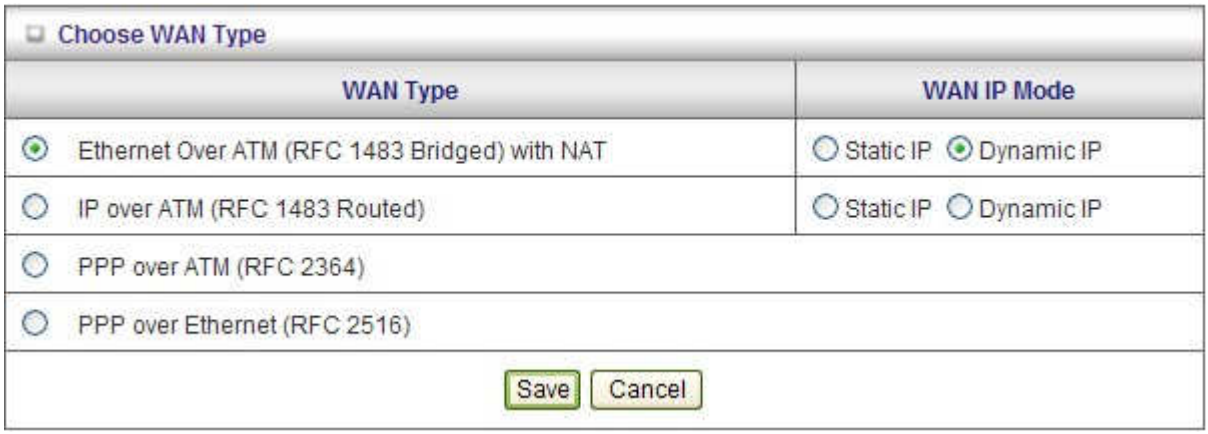
Primary Setup

This page lets you change the LAN (Local Area Network) settings on your WBR-6603 150Mbps Wireless ADSL2+ Modem Router and WAN (Wide Area Network) connection.



1. **LAN IP Address:** The local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.

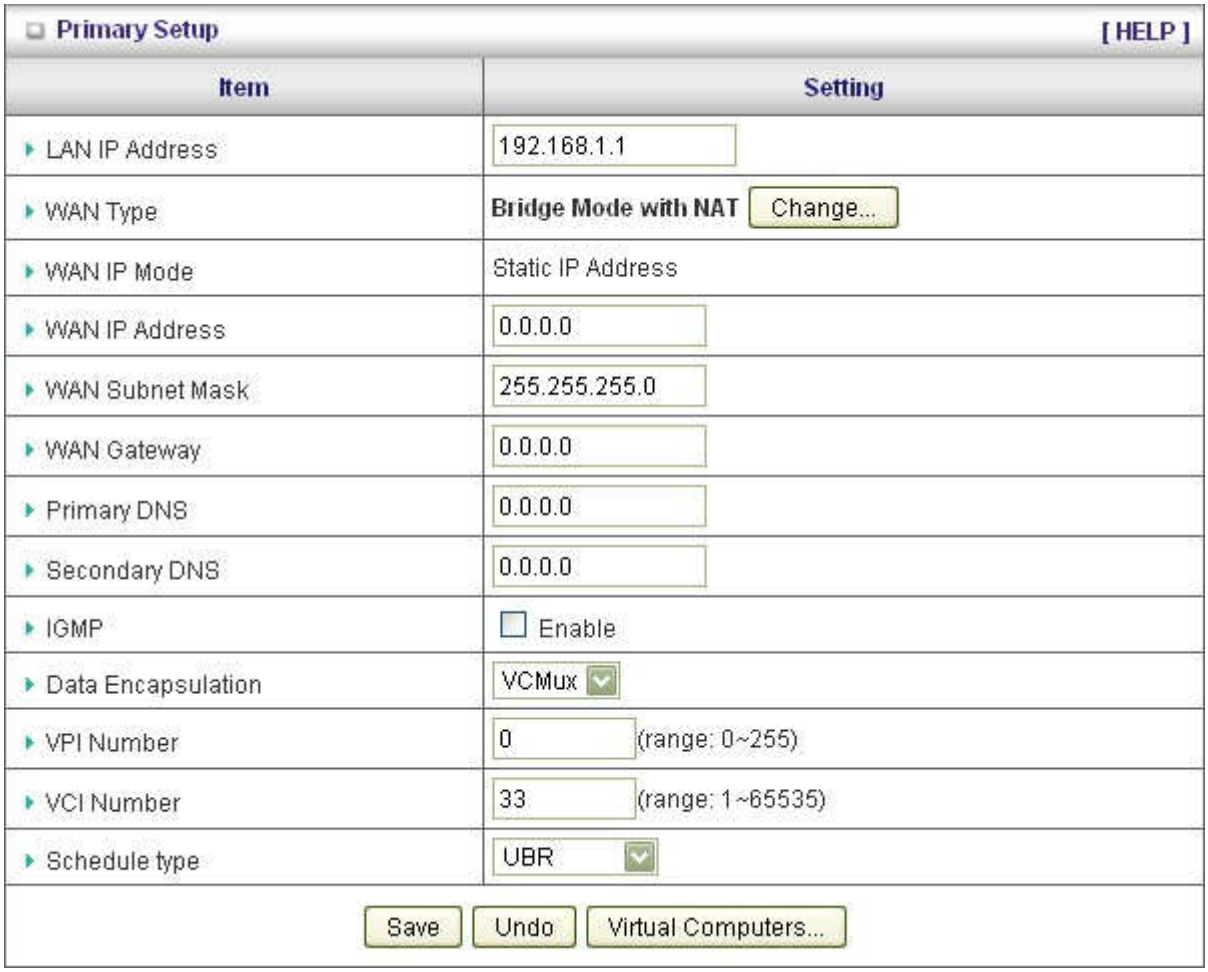
2. **WAN Type:** WAN connection type of your ISP. You can click the **Change** button to choose the most suitable one from the following options:



This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. You can choose a correct one from the following options:

A. Ethernet Over ATM (RFC 1483 Bridged) with NAT
B. IP over ATM (RFC 1483 Routed).
C. PPP over ATM (RFC 2364).
D. PPP over Ethernet (RFC 2516).

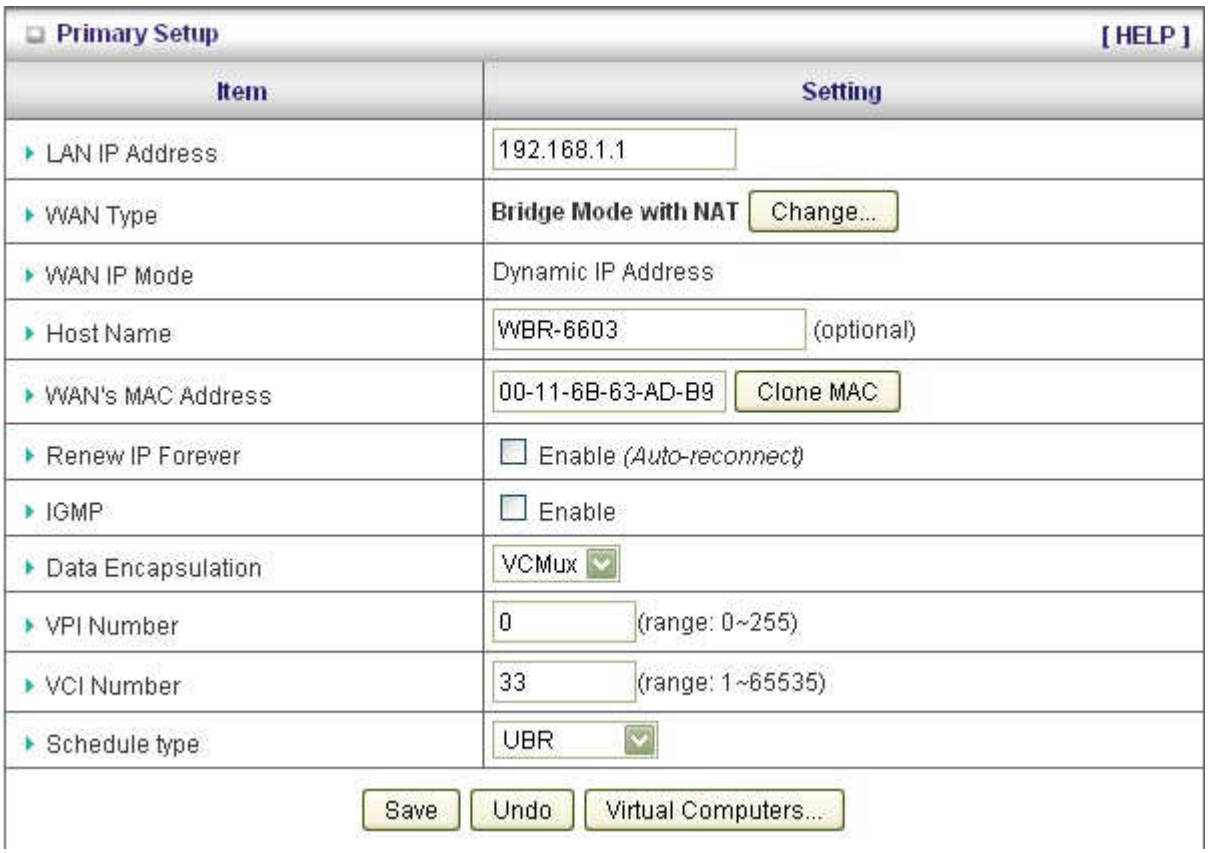
A. Ethernet Over ATM with Static IP Address



1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS:**

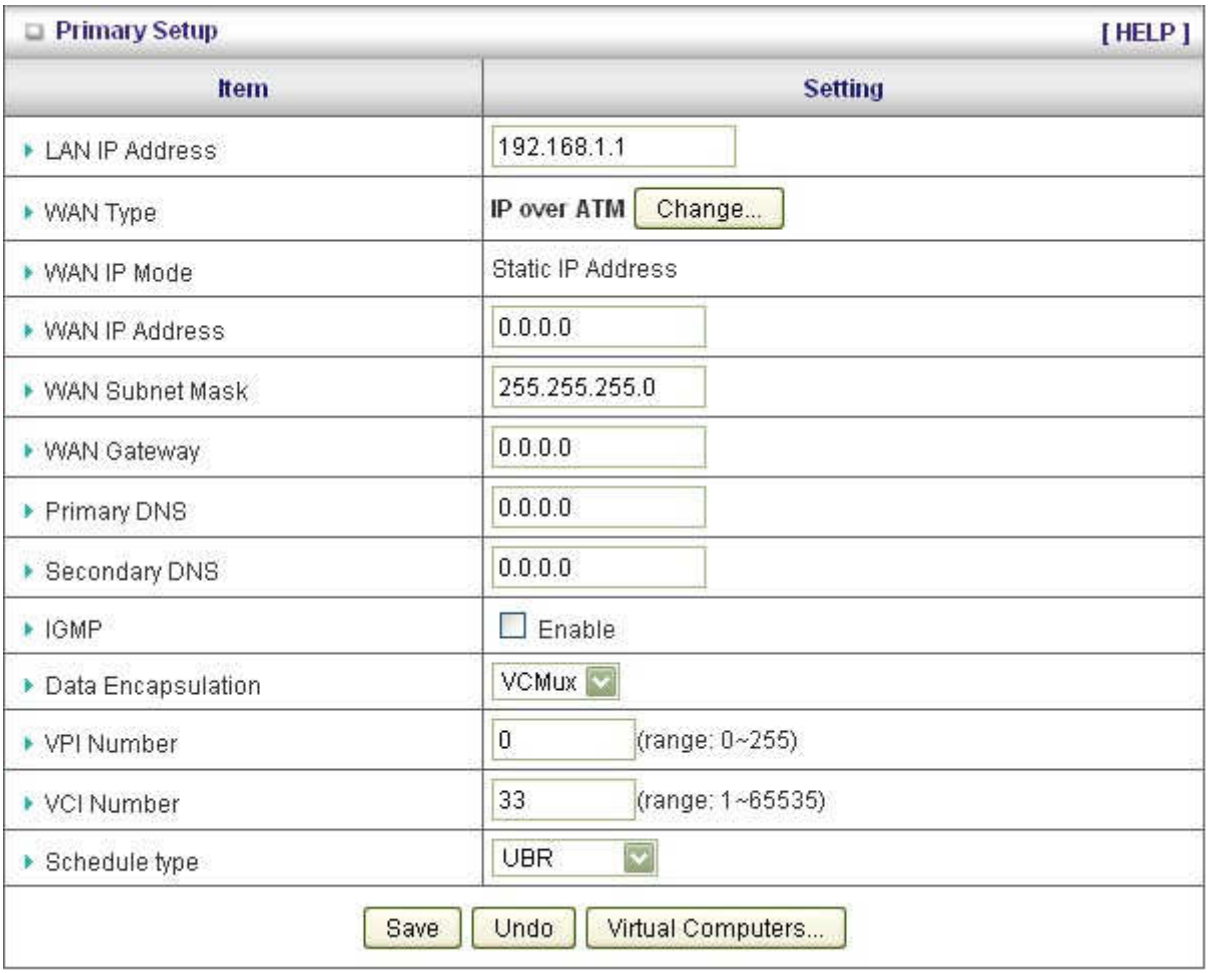
   Enter the proper settings provided by your ISP.
3. **IGMP :** If you enable this option, the device would allow IGMP packet pass through.
4. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
5. **VPI and VCI, Schedule Type:** These values depend on your ISP setting.

B. Ethernet Over ATM with Dynamic IP Address



1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **Host Name:** The name that shown on client list at server side.
3. **WAN's MAC Address:** You can manually setup the WAN's MAC address by clicking the **Clone MAC** button.
4. **Renew IP Forever:** This feature allows this product renew IP address automatically when the lease time is being expired even the system is in idle state.
5. **IGMP:** If you enable this option, the device would allow IGMP packet pass through.
6. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
7. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.

C. IP Over ATM with Static IP Address



1 **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.

2 **WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS**:

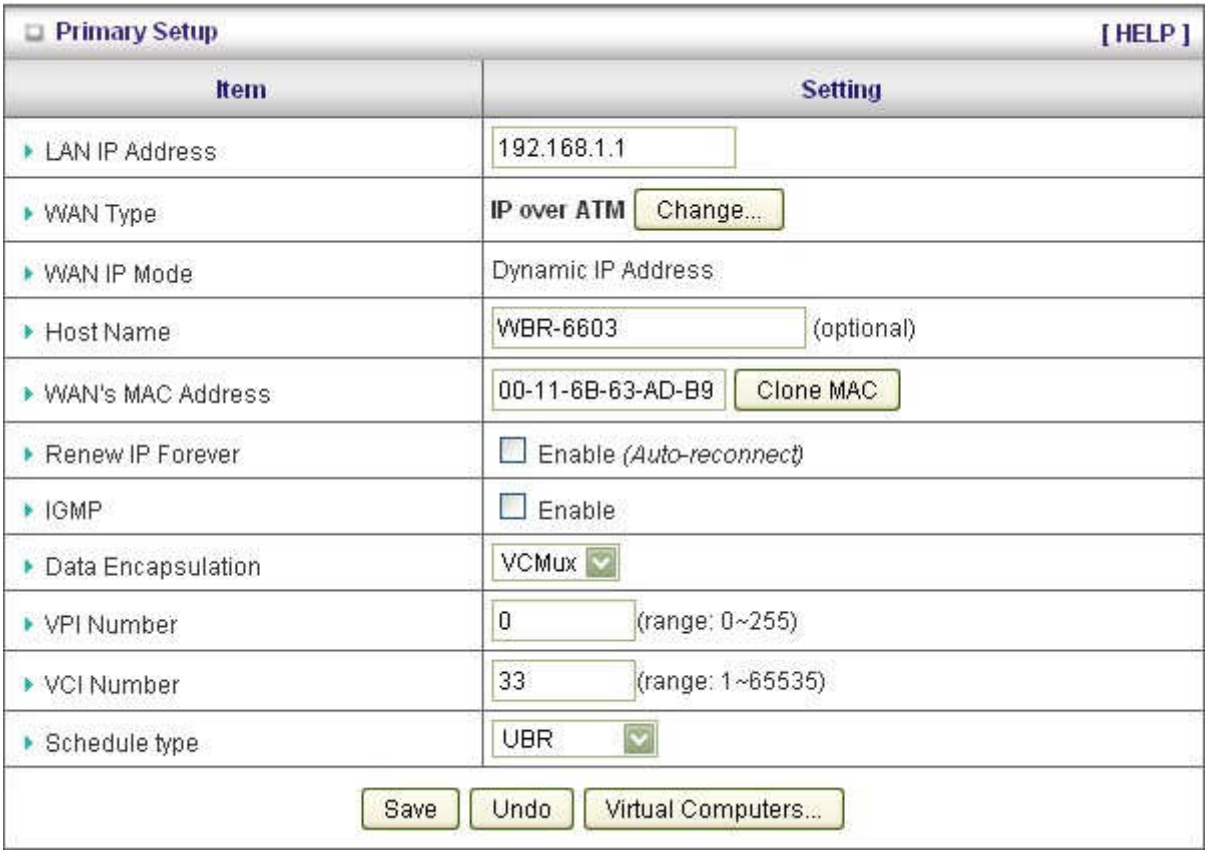
Enter the proper settings provided by your ISP.

3 **IGMP:** If you enable this option, the device would allow IGMP packet pass through.

4 **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.

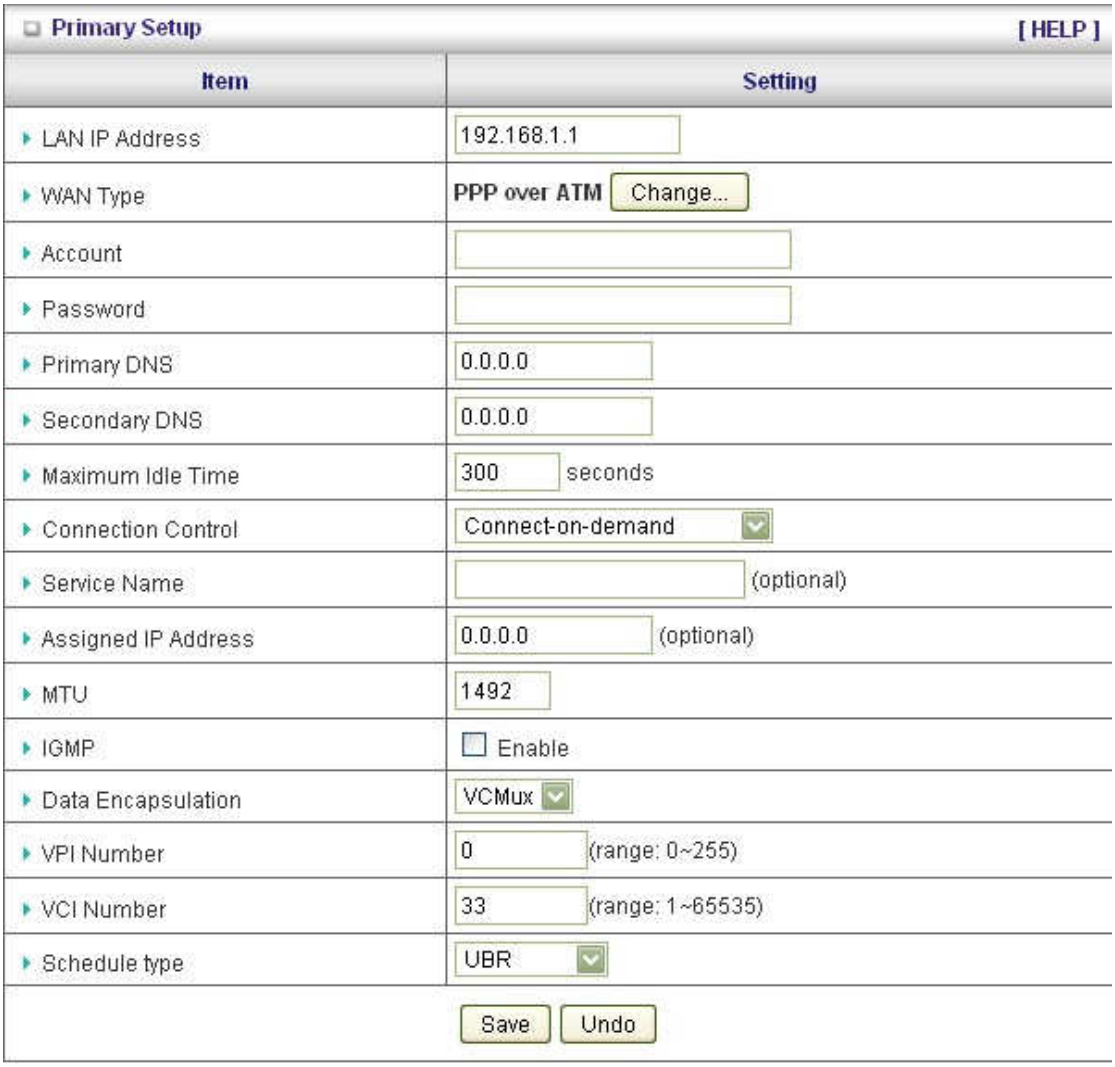
5 **VPI and VCI, Schedule Type:** these values depend on your ISP setting.

D. IP Over ATM with Dynamic IP Address



1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **Host Name:** The name that shown on client list at server side.
3. **WAN's MAC Address:** You can manually setup the WAN's MAC address by clicking the **Clone MAC** button.
4. **Renew IP Forever:** This feature allows this product renew IP address automatically when the lease time is being expired even the system is in idle state.
5. **IGMP:** If you enable this option, the device would allow IGMP packet pass through.
6. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
7. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.

E. PPP Over ATM



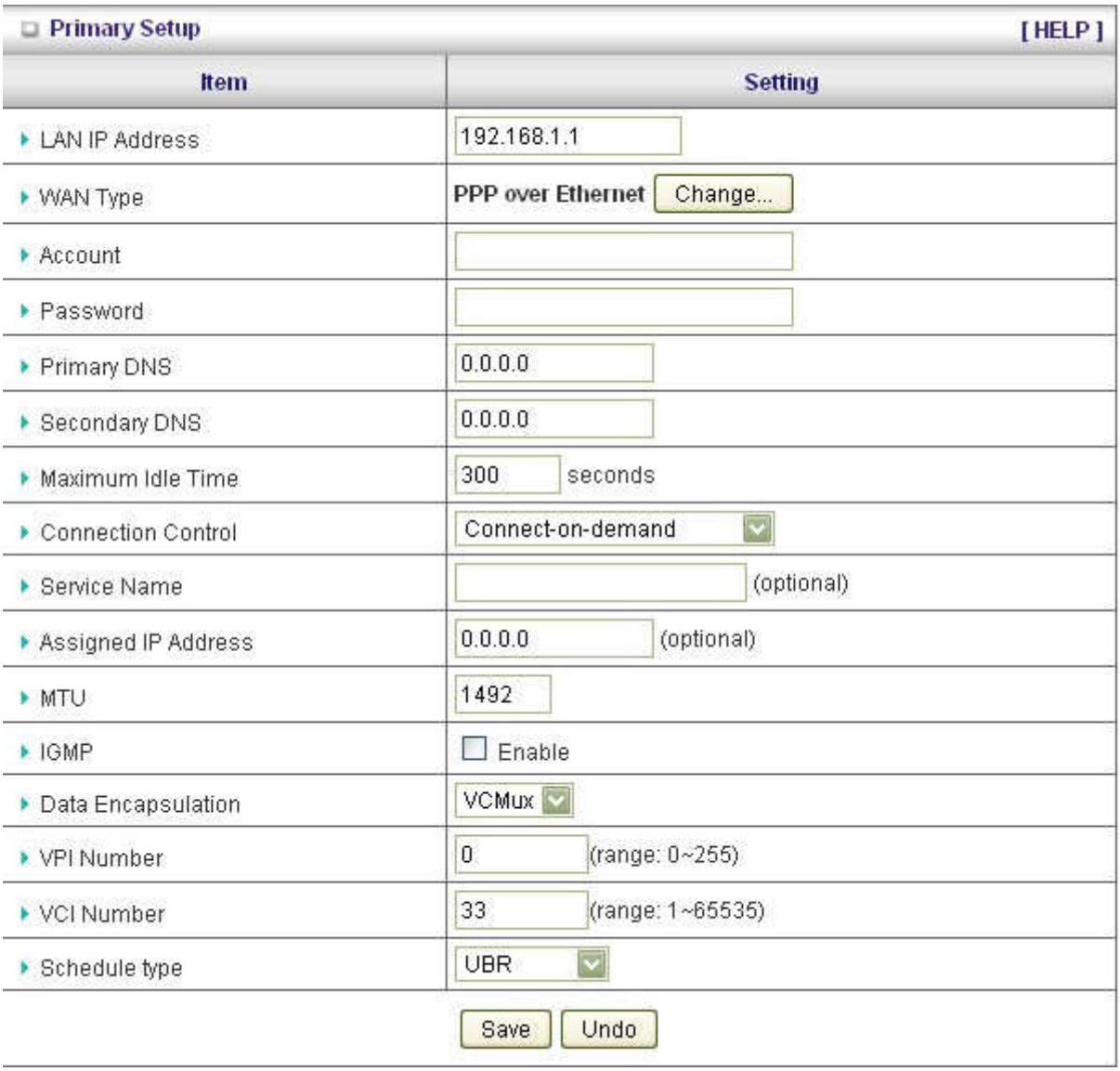
1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **PPPoA Account , Password, Primary and Secondary DNS**: Enter the proper settings provided by your ISP.
3. **Maximum Idle Time**: the time of no activity to disconnect your PPPoA session. Set it to zero or enable "Auto-reconnect" to disable this feature. If Auto-reconnect is enabled, this device will connect with ISP automatically after system is restarted or connection is dropped.
4. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
5. **Service Name:** Sometimes your ISP would give you a specified service name to dial-up.
6. **Assigned IP Address:** If your ISP provides you a specified IP address, fill it here.
7. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The default MTU value is 0 (auto).
8. **IGMP:** If you enable this option, the device would allow IGMP packet pass through.
9. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
10. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.

F. PPP Over Ethernet



1. **PPPoE Account** and **Password**: The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
2. **Primary and Secondary DNS:** Enter the proper settings provided by your ISP.
3. **Maximum Idle Time**: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable "Auto-reconnect" to disable this feature.
4. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

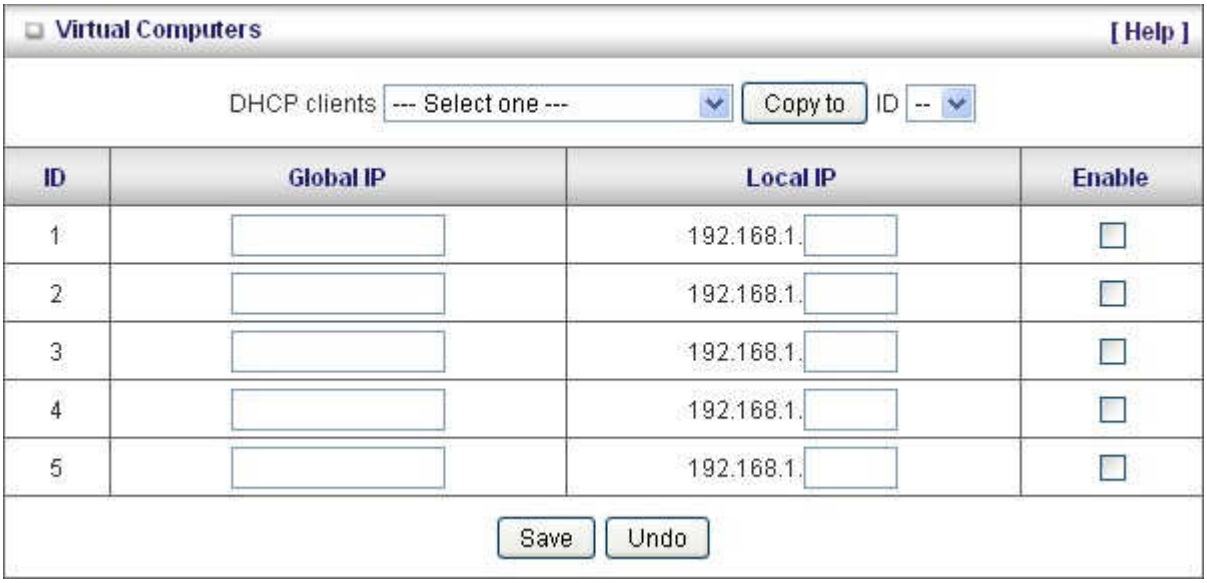
   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
5. **Service Name**: Optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
6. **Assigned IP Address:** It is required by some ISPs. (Optional)
7. **Maximum Transmission Unit (MTU):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
8. **IGMP:** If you enable this option, the device would allow IGMP packet pass through.
9. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
10. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

Virtual Computers (Only for Static and dynamic IP address WAN type)

Used when WAN is set as DHCP or Static IP, user can assign a global IP address to a LAN IP Address.

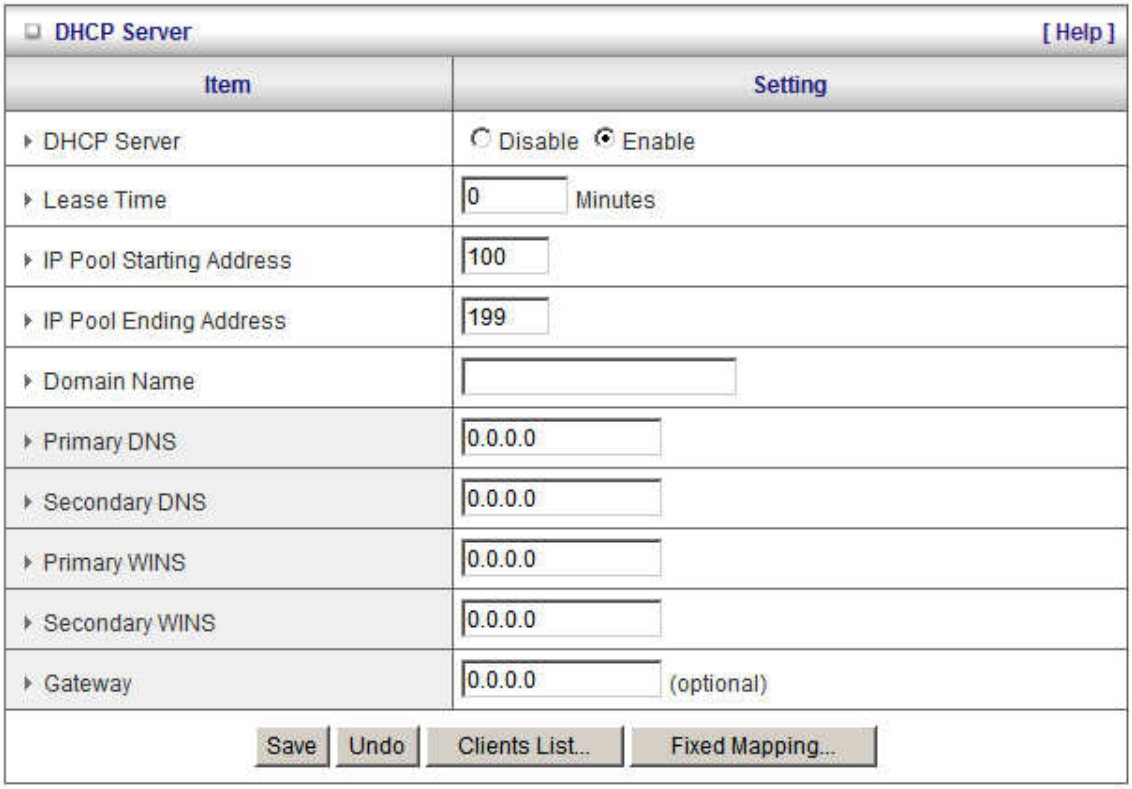


Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

- **Global IP:** Enter the global IP address assigned by your ISP.
- **Local IP:** Enter the local IP address of your LAN PC corresponding to the global IP address.
- **Enable:** Check this item to enable the Virtual Computer feature.

DHCP Server

This page allows you to configure the DHCP server on the *150Mbps Wireless ADSL2+ Modem Router*



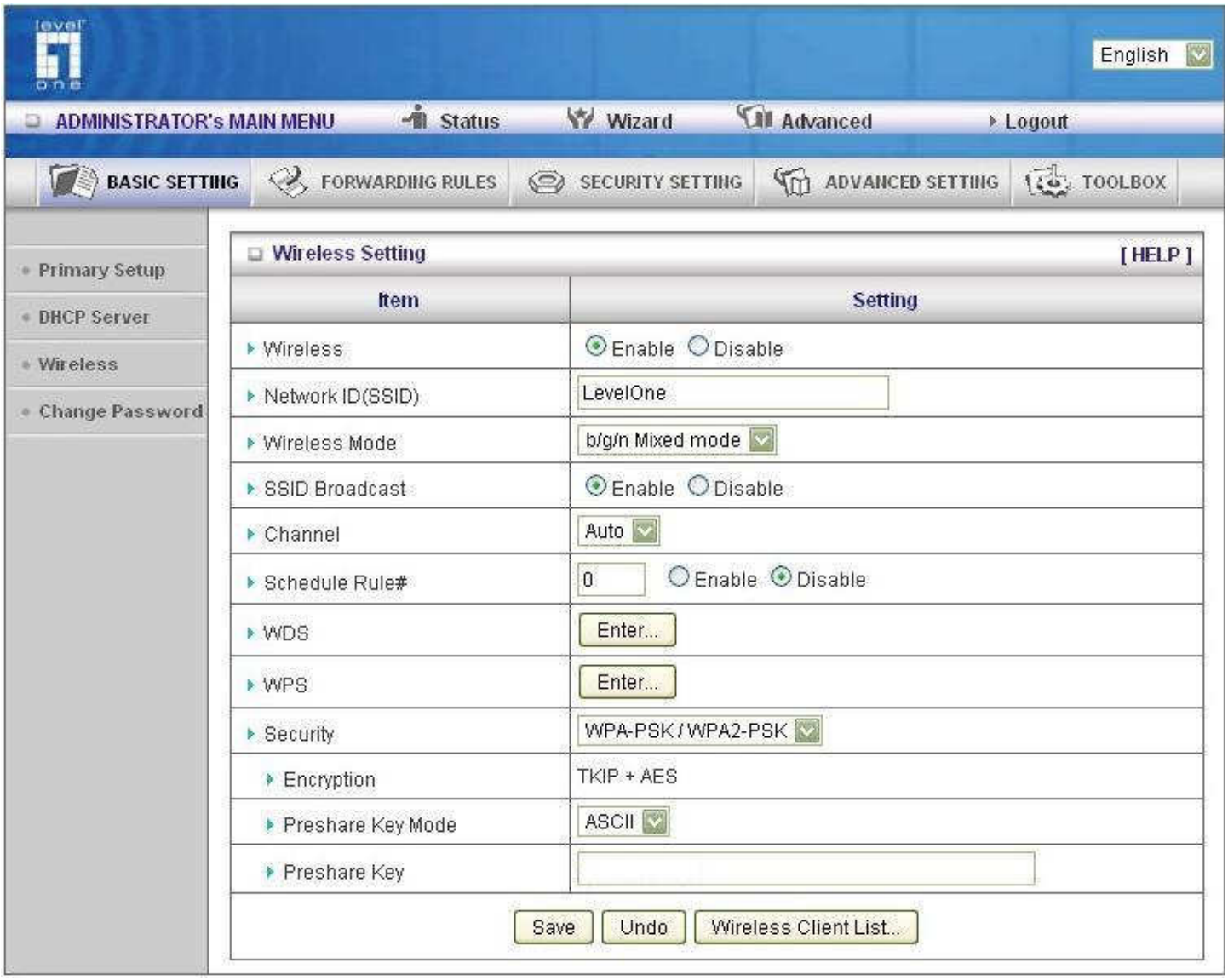
For more settings click on **More**.

DHCP Server: To either Disable or Enable DHCP Server.
Lease Time: DHCP lease time to the DHCP client
IP Pool Starting/Ending Address: The pool of IP's that can be allocated to clients
Domain Name: To assign a Domain Name (optional)
Primary DNS/Secondary DNS: To assign DNS Servers (optional)
Primary WINS/Secondary WINS: To assign WINS Servers (optional)
Gateway: The IP address of an alternate gateway (optional)

Clients List: Check the DHCP client list.
Fixed Mapping: Take you to the Security > MAC Control page. (see page 52)

After you finish your selections click either **Save** to store your settings, or **Undo** to exit.

Wireless Settings



Wireless: Enabled by default. Disabling this feature will turn off the wireless function of this unit.

Network ID (SSID): Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **LevelOne**. The SSID can be easily changed to establish a new wireless network.

Note: SSID names may contain up to 32 ASCII characters.

Wireless Mode: You can choose the wireless mode to IEEE 802.11b/g/n Mixed mode, b/g Mixed mode, g/n Mixed mode, IEEE 802.11b only, IEEE 802.11g only, or IEEE 802.11n only.

SSID Broadcast: The WBR-6603 will broadcast beacons that contains SSID and other wireless information so that Computers or other wireless devices can find the WBR-6603 when scanning for wireless networks. Disable this function if you want to hide your wireless network.

Channel: The radio channel number. The permissible channels depend on the Regulatory Domain. The default is AUTO which means the WBR-6603 will find the least used channel to avoid interference.

Note:
Channel range depends on your regional regulations. Please see specifications for Channel details.

Schedule Rule: You can Enable / Disable wireless by schedule rule, and setup the Schedule rules numbers you want to apply in list. For further setting please see **"page 61" Schedule Rule.**

WPS (WiFi Protected Setup)

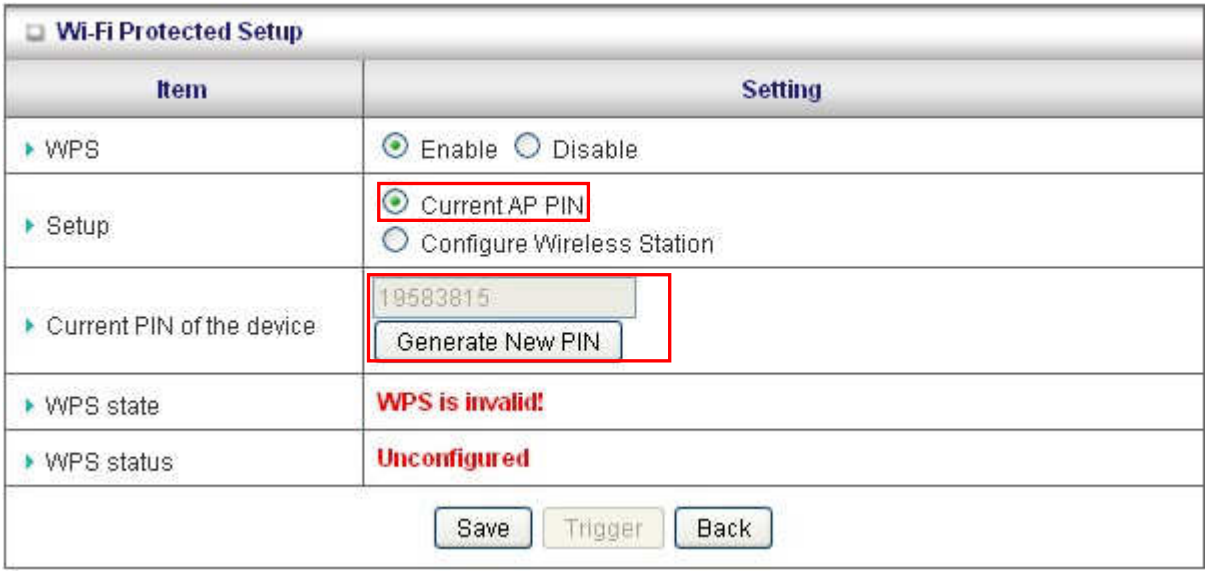
WPS feature is following the Wi-Fi Alliance WPS standard and it eases the set up of security-enabled Wi-Fi networks in the home and small office environment.

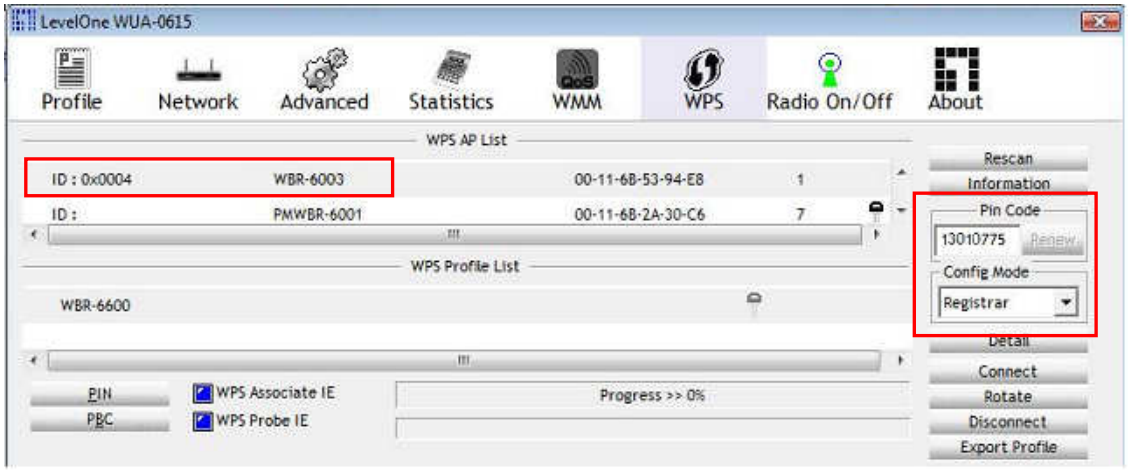
It reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

Please ensure you have wireless security set up on the WBR-6603 before initializing WPS functions.

Set PIN number of WBR-6603
Click the "Generate New PIN" button to randomly create a new PIN number for the WBR-6603.

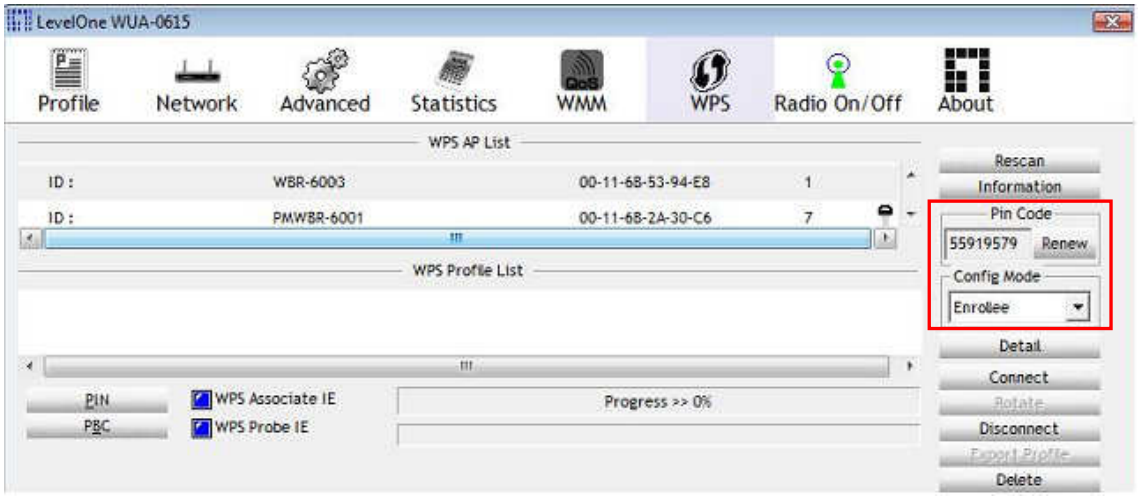
Set your wireless adapter as Registrar and enter this PIN number to initiate the WPS function.



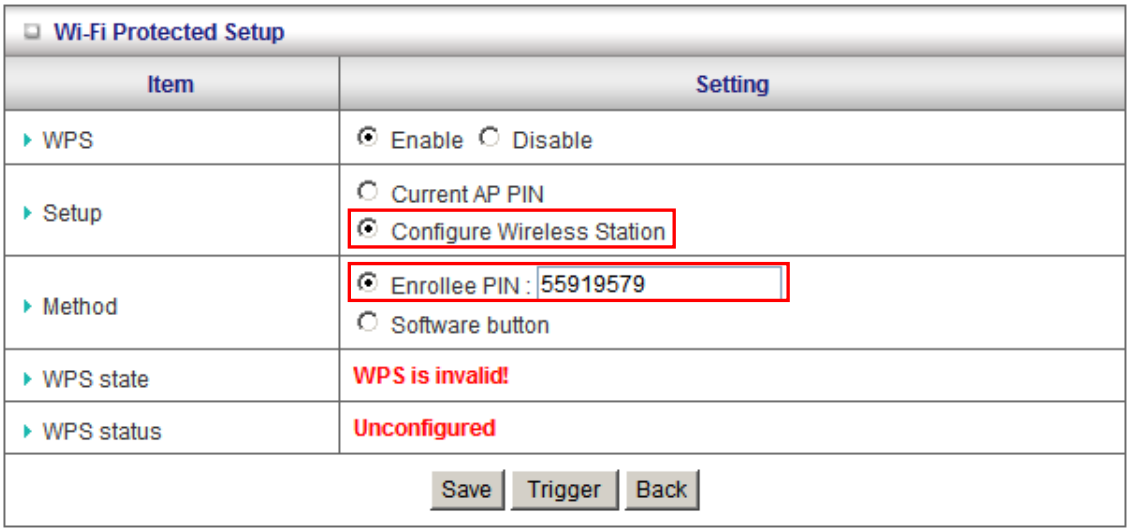


Enter PIN number of Wireless Adapter

It is also possible to use the PIN number you have set on the wireless adapter. Set the adapter as Enrollee and enter the PIN you want.

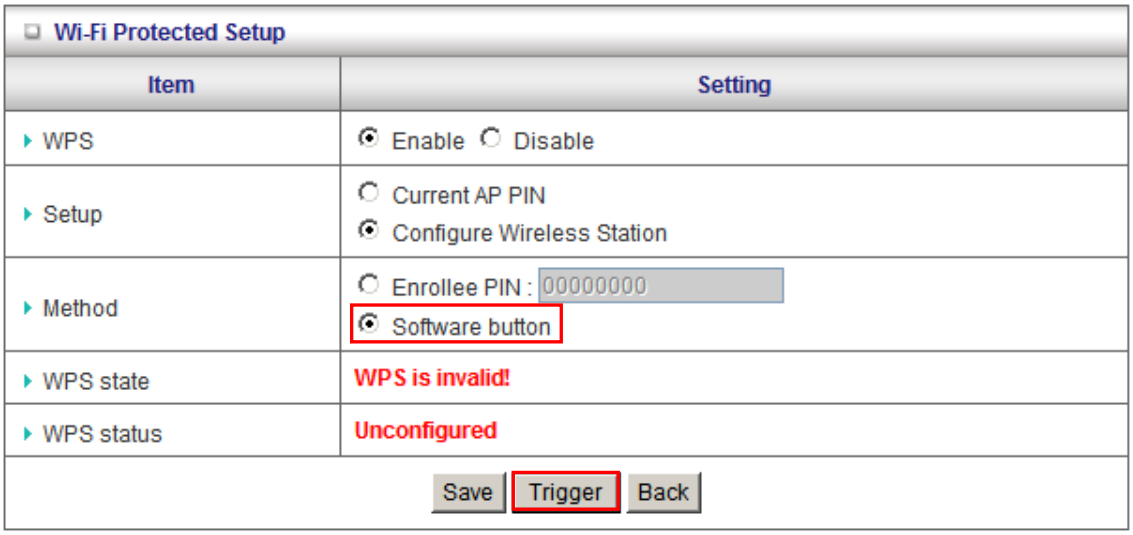


Enter the enrollee's (computer's wireless adapter) PIN number and then click the "Trigger" button to initiate WPS.

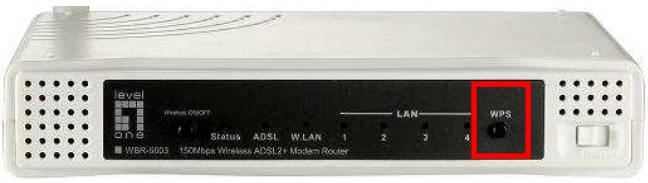


Push Button Method

Select the “Software Button” mode and click the “Trigger” button.

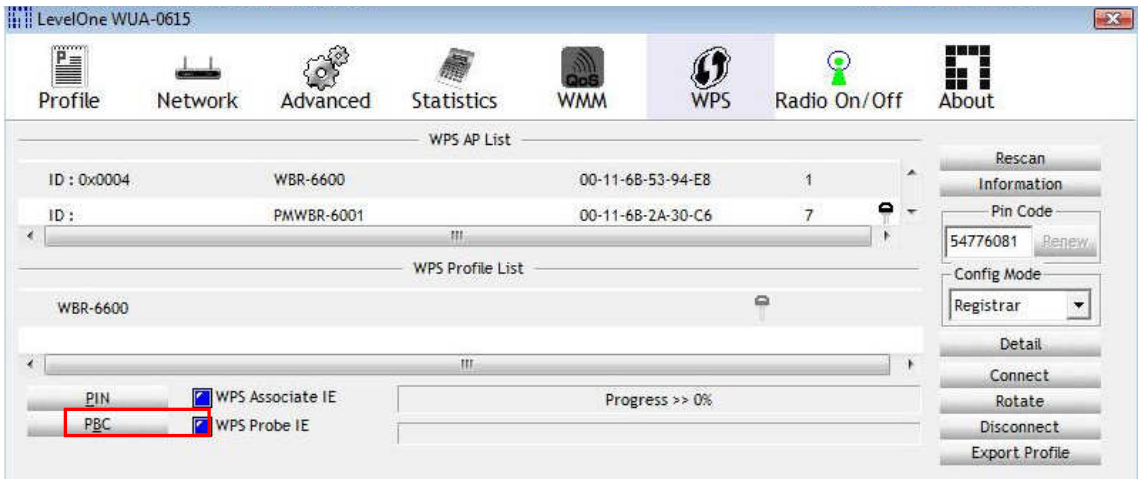


An alternative is to press the WPS button at the front of the router for 1 second, until the WLAN light starts flashing. This indicates that WPS is activated.



Then press and hold the WPS button on your wireless client for 1 second.

If your device has no physical WPS push button, then you can push the software button in the utility.



WDS (Wireless Distribution System)

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

For maximum compatibility, it is recommended that WDS be set up using only the same models, in this case, WBR-6603. Also note that the standard only supports WEP encryption.

Select the AP Mode that most suites your desired application.

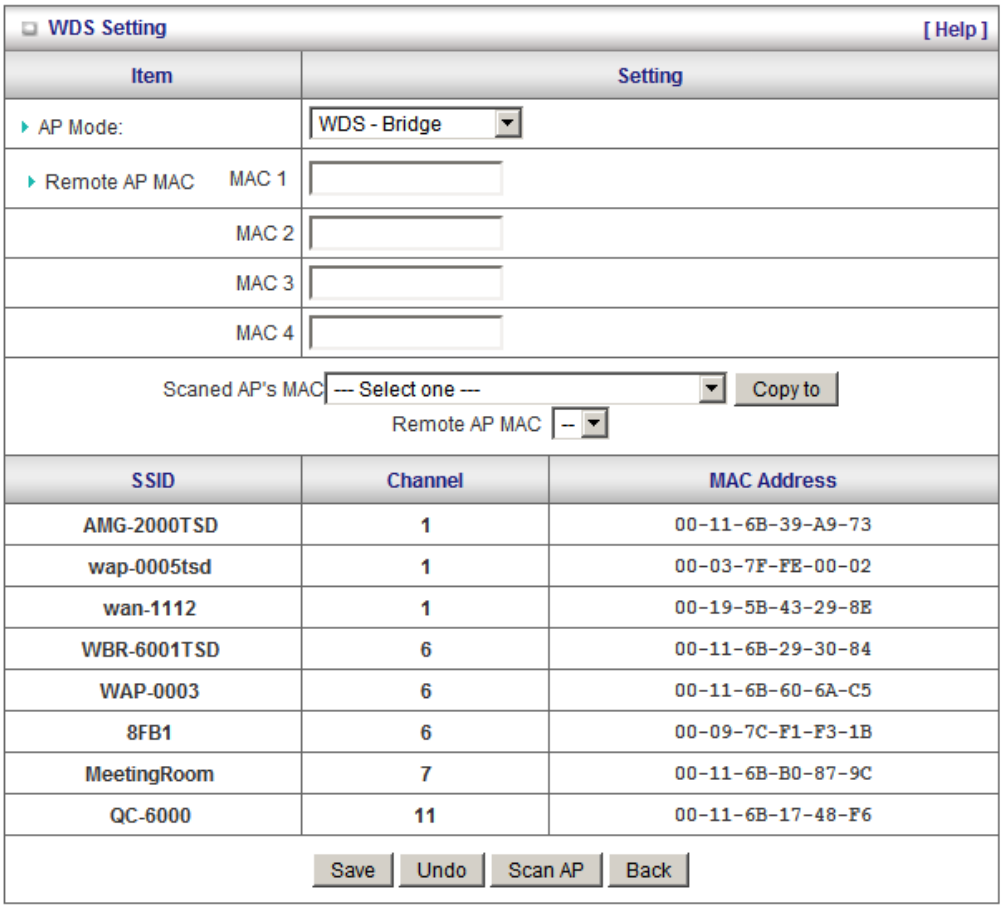
AP Only:
WDS is disabled. WBR-6603 functions as normal Access Point mode

WDS Only:
Create a WDS Bridge between multiple Access Points, and bridge to only wired connections. In this mode, the WBR-6603 will not provide service to any wireless clients.

Hybrid mode:
A combination of the AP and Bridge modes can create a WDS Bridge between multiple Access Points, and also accept wireless and wired clients.

Then type in the MAC addresses of other Access Points in the **Remote AP MAC** fields. Or you can copy the ones from **Scanned AP's MAC** list.

Click **Save** to save the settings and **Undo** to cancel.



Security: Security - You may select from three levels of encryption to secure your wireless network: No Encryption, WEP, 802.1x RADIUS, WPA-PSK, WPA, WPA2-PSK (AES), WPA2 (AES), WPA-PSK / WPA2-PSK and WPA1 / WPA2.

LevelOne recommends **WPA2-PSK (AES)** for simple and secure wireless encryption.

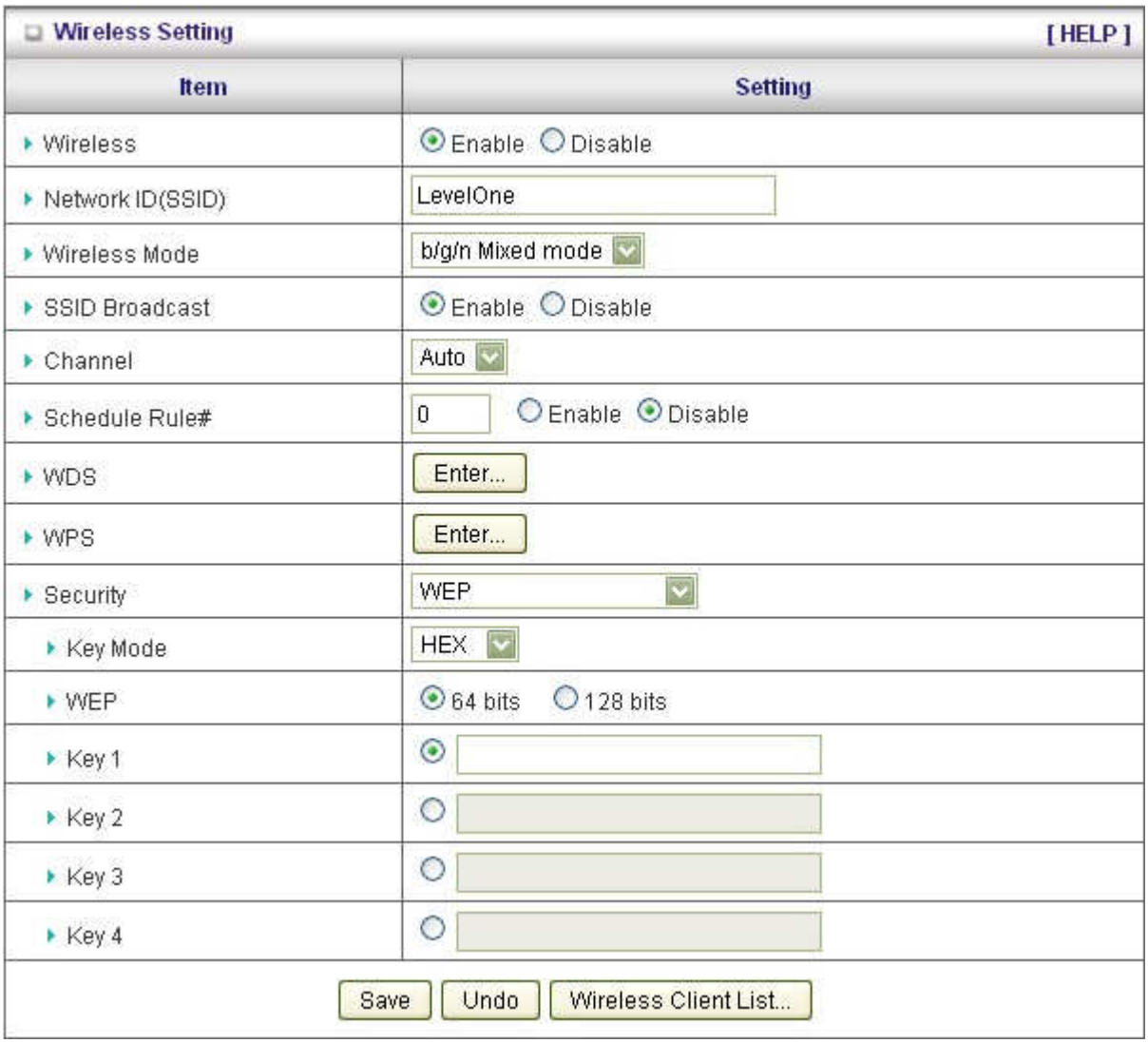
After configuring the wireless security settings on the WBR-6603, you will also need to configure the same settings on your wireless adapter before you attempt a wireless connection.

Please note that not all adapters support all the available security functions.

No Encryption is the default (as shown in the screen above).

WEP:

WEP (Wired Equivalent Privacy). Enabling the security can protect your data while it is transferred to the WBR-6603. Select the WEP Encryption (64bit or 128bit) and enter the WEP key. Please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.



802.1X

To use this security feature, you will need to have a RADIUS server on your network to authenticate access. Please type in the details for your RADIUS server.

RADIUS Server IP

Please enter your RADIUS server IP Address.

Radius port

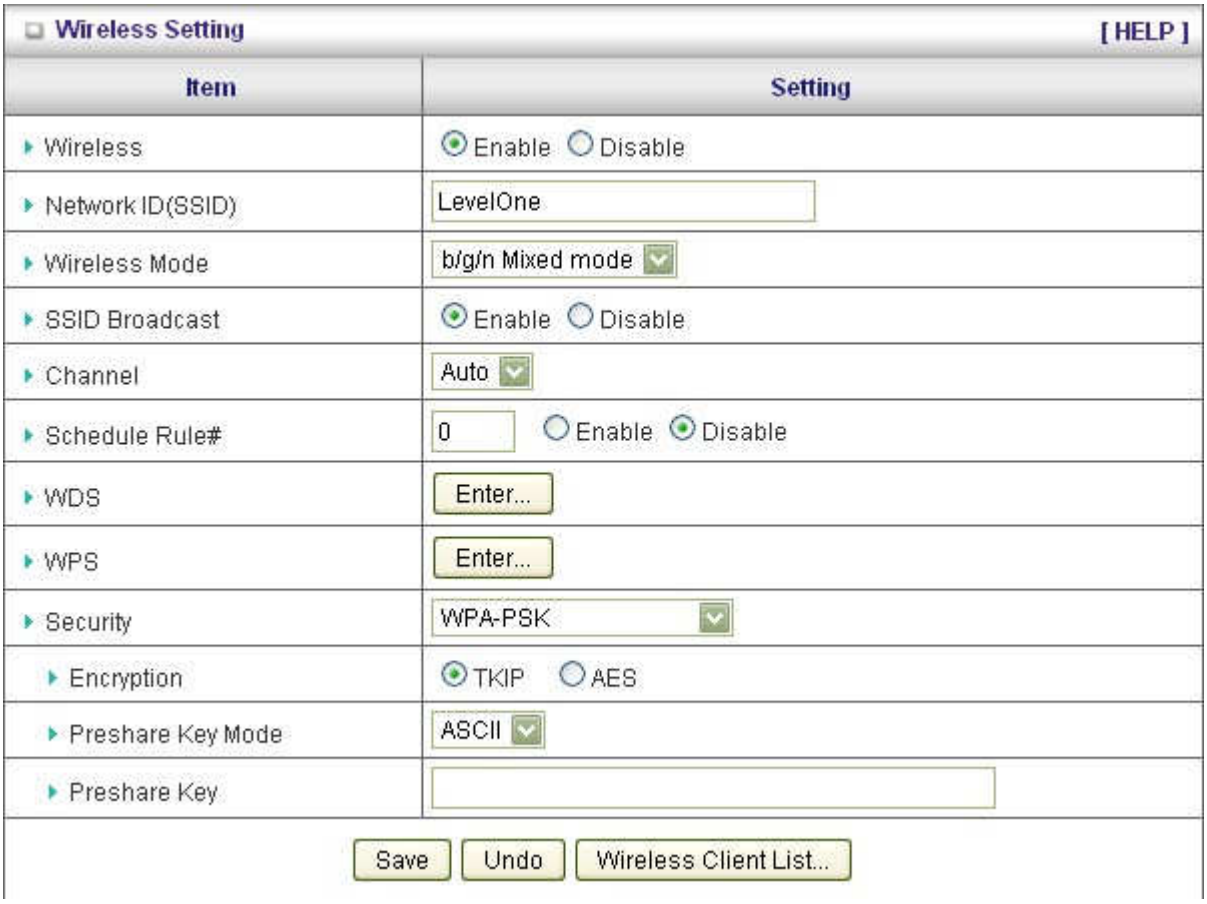
You can change RADIUS server port by manually.

RADIUS Shared Key

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK

This security is more secure compared to WEP. Select which type of encryption to use (either TKIP or AES) and then enter the key in the Passphrase field. The field needs to be between 8 and 63 characters long and can be any combination of letters and numbers if **ASCII** setting is used.



WPA, WPA2(AES) WPA1/WPA2

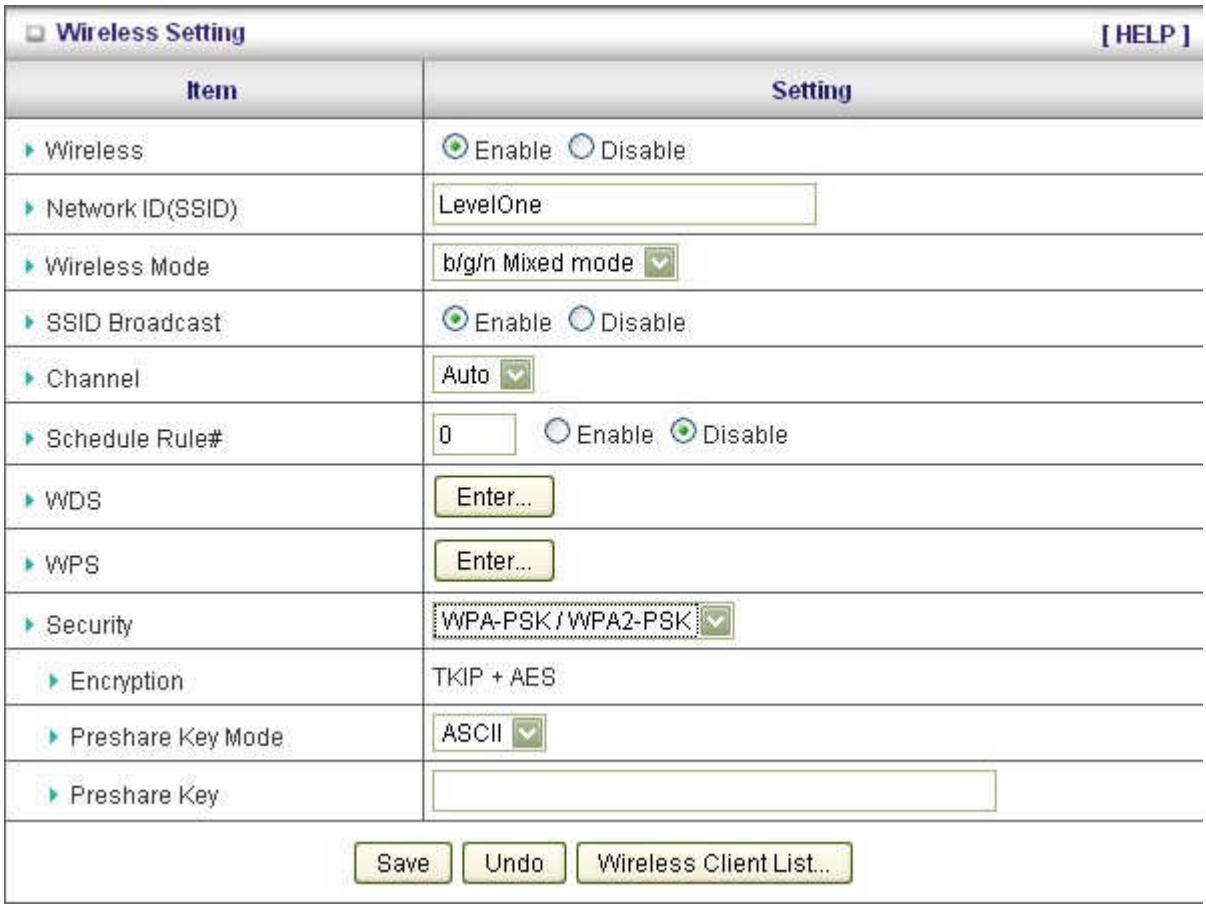
Similar to 802.1X security but with TKIP or AES Encryption. You will need a RADIUS server for authentication. Please enter the details of your RADIUS server.

RADIUS Server

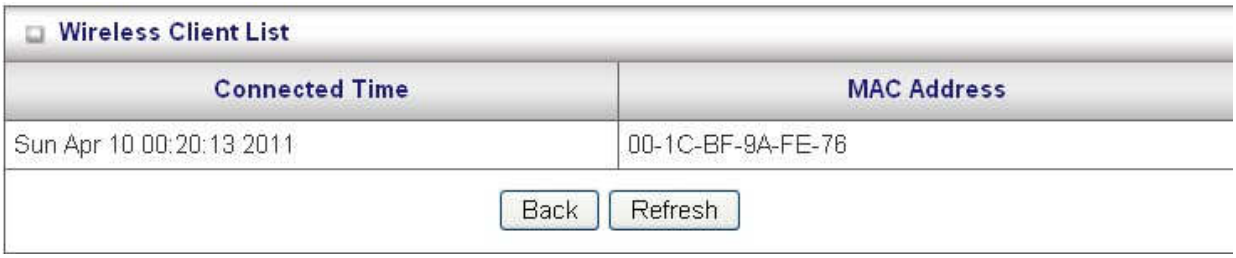
- IP address or the RADIUS server's IP address.
- Port number of the RADIUS Server
- Enter the RADIUS Shared Key
  Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK, WPA2-PSK(AES), WPA / WPA2-PSK

This security is more secure compared to WEP. It will use either TKIP or AES for enhanced security. Please enter the key in the Passphrase field. The field can be between 8 and 63 characters long and can be any combination of letters and numbers under **ASCII** format.



Wireless Client List: You can use this function to see the devices connected to the WBR-6603 through the wireless network.



Change Password

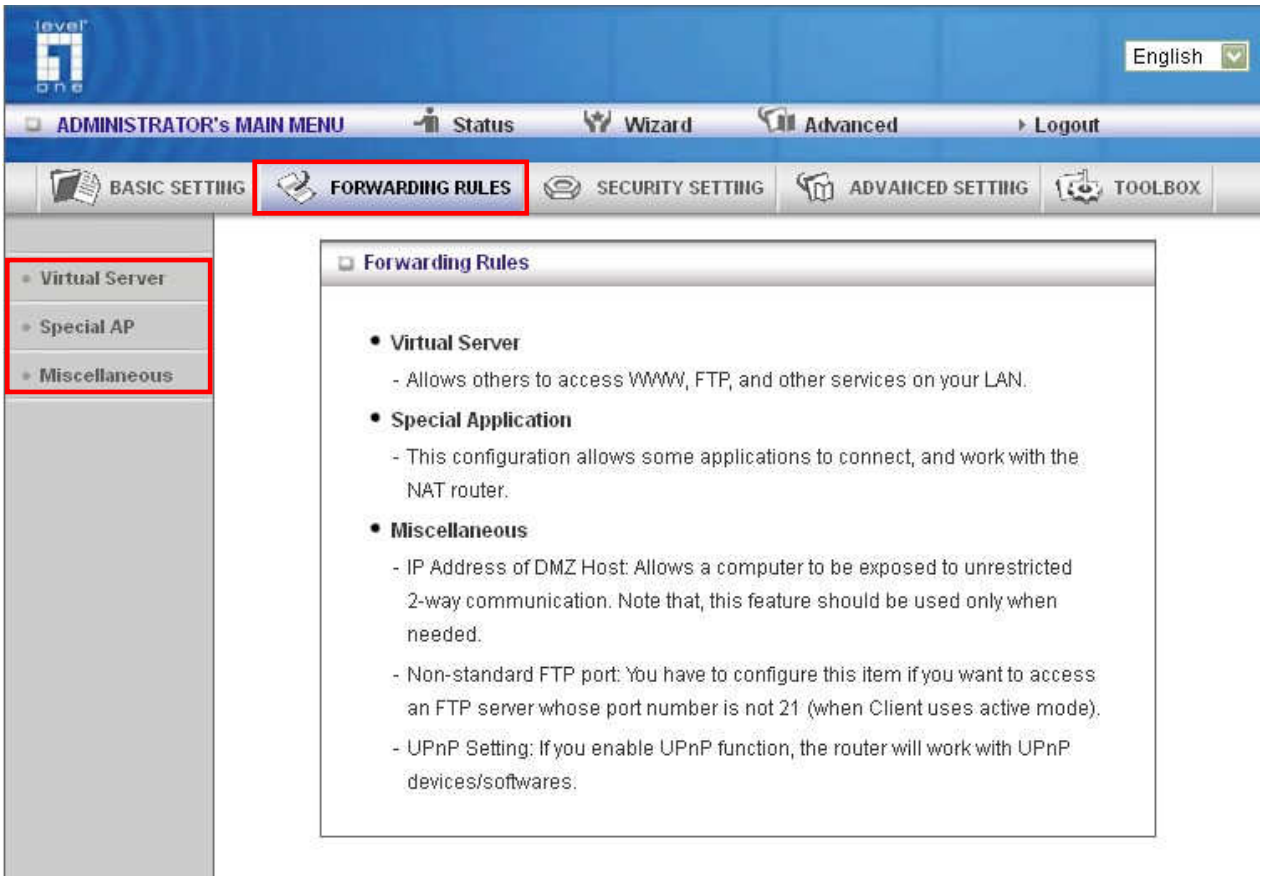
This page allows you to change the WBR-6603 Web Configuration password. Please type in the old password (factory default password is **admin**) and then type in the new password.

If you change the password, make sure you use the new password next time you login the web configuration page.

Click **Save** to save the settings and **Undo** to cancel.

Forwarding Rules

This page allows you to configure the port forwarding management of the WBR-6603. Use the menu on the left to access the setting pages.

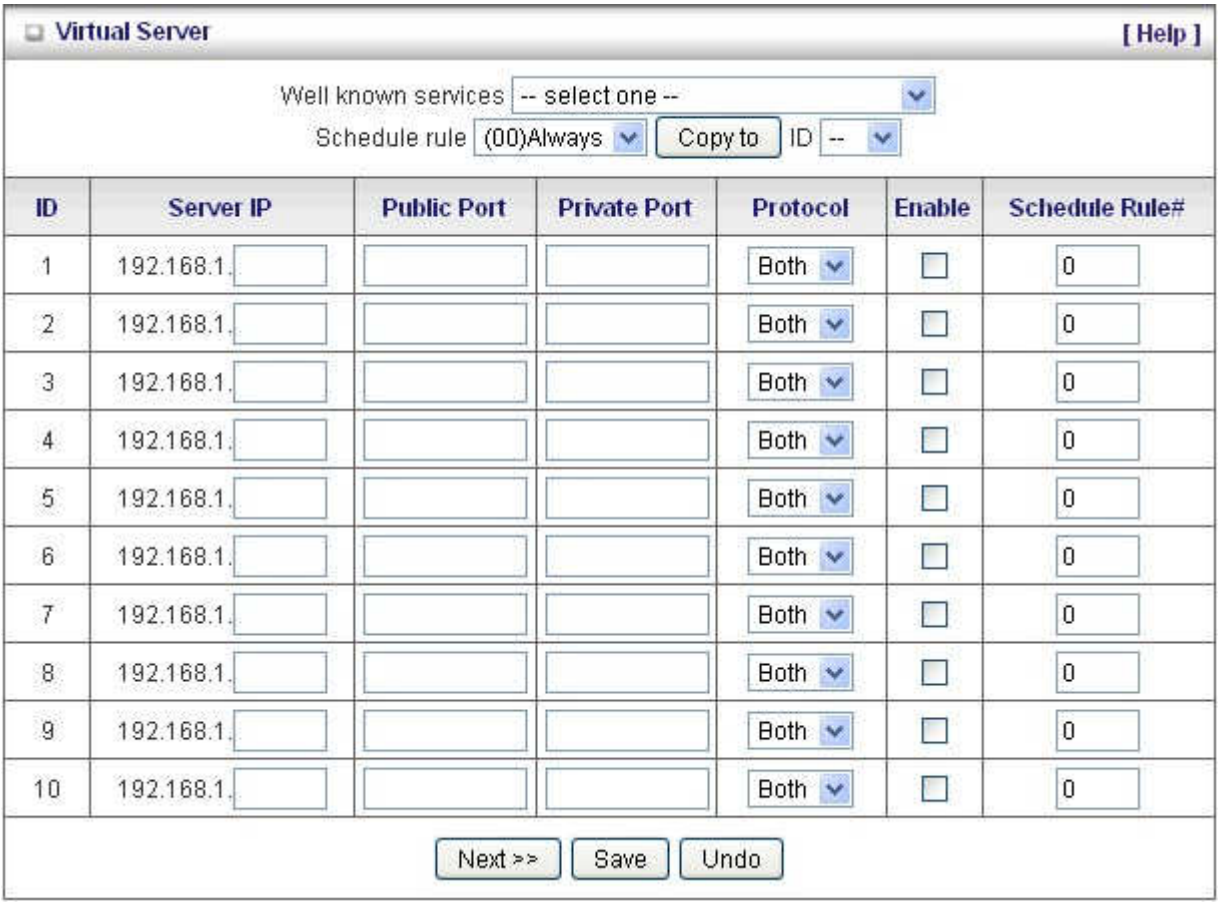

English
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
Virtual Server
Special AP
Miscellaneous
Forwarding Rules
Virtual Server
- Allows others to access WWW, FTP, and other services on your LAN.
Special Application
- This configuration allows some applications to connect, and work with the NAT router.
Miscellaneous
- IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
- Non-standard FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode).
- UPnP Setting: If you enable UPnP function, the router will work with UPnP devices/softwares.

The port forwarding feature is required because the ADSL Router's NAT (Network Address Translation) will block incoming traffic from the Internet to the LAN if the specific port mapping is not set up in the NAT table.

This is to provide a level of protection to computers on your LAN, however as a result creates connectivity problems when you want to make LAN resources available on the Internet. These include FTP servers, network game servers or other server applications.

There are three ways to work around the NAT and enable LAN resources on the Internet. Port Forwarding (Virtual Server), Port Triggering (Special AP page) and DMZ Host (Miscellaneous page).

Virtual Server


Virtual Server
[Help]
Well known services -- select one --
Schedule rule (00)Always Copy to ID --
ID Server IP Public Port Private Port Protocol Enable Schedule Rule#
1 192.168.1. Both 0
2 192.168.1. Both 0
3 192.168.1. Both 0
4 192.168.1. Both 0
5 192.168.1. Both 0
6 192.168.1. Both 0
7 192.168.1. Both 0
8 192.168.1. Both 0
9 192.168.1. Both 0
10 192.168.1. Both 0
Next >> Save Undo

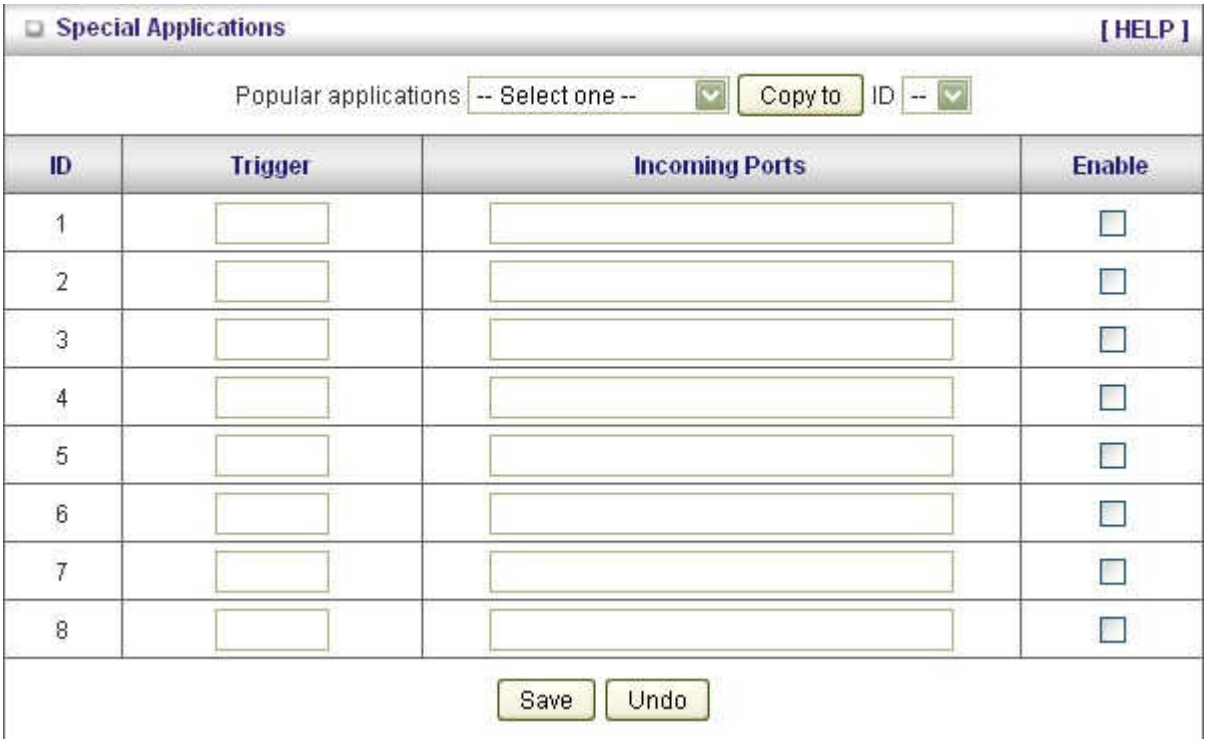
A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. Virtual Server can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule (Advanced Setting > Schedule Rule).

For example, if you have an FTP server (port 21) at 192.168.1.2, a Web server (port 80) at 192.168.1.3, and a VPN server at 192.168.1.6, then you need to specify the following virtual server mapping table:

You can specify different ports to be used for Public and Private source and destinations.

Public Port	Private Port	Server IP	Enable
21	21	192.168.1.2	V
80	80	192.168.1.3	V
1723	1723	192.168.1.6	V

Special AP



Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with the WBR-6603. The **Special Applications** feature allows some of these applications to work with this product. If this fails to make an application work, try setting that computer as the **DMZ host** instead. Please refer to Forwarding Rules > Miscellaneous section.

1. **Trigger:** The outbound port number that will be triggered by the application.
2. **Incoming Ports:** When the trigger packet is detected, the inbound packets sent to the specified port numbers and are allowed to pass through the firewall.

The WBR-6603 also comes with predefined settings for some popular applications. To use the predefined settings, select your application from the list, select an unused ID and then click **Copy** to add the predefined setting to your list.

Note: At any given time, only one PC can use each Special Application tunnel.

Miscellaneous

-

Miscellaneous Items		[Help]
Item	Setting	Enable
IP Address of DMZ Host	192.168.1.	☐
Non-standard FTP port		
UPnP setting		☑
Xbox Support		☑
Save Undo		

IP Address of DMZ Host

DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

To enable DMZ, enter the IP address of the PC and tick on Enable.

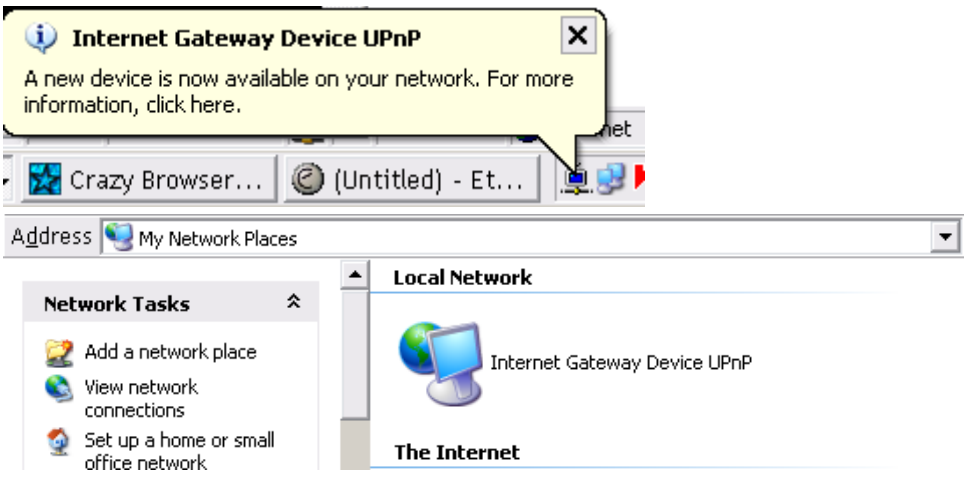
NOTE: This feature should be used only when needed

Non-standard FTP port

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

UPnP Setting

The WBR-6603 supports Universal Plug and Play. If the OS supports this function enable it likes Windows XP. When the user gets IP address from Device, it will show icon as below:

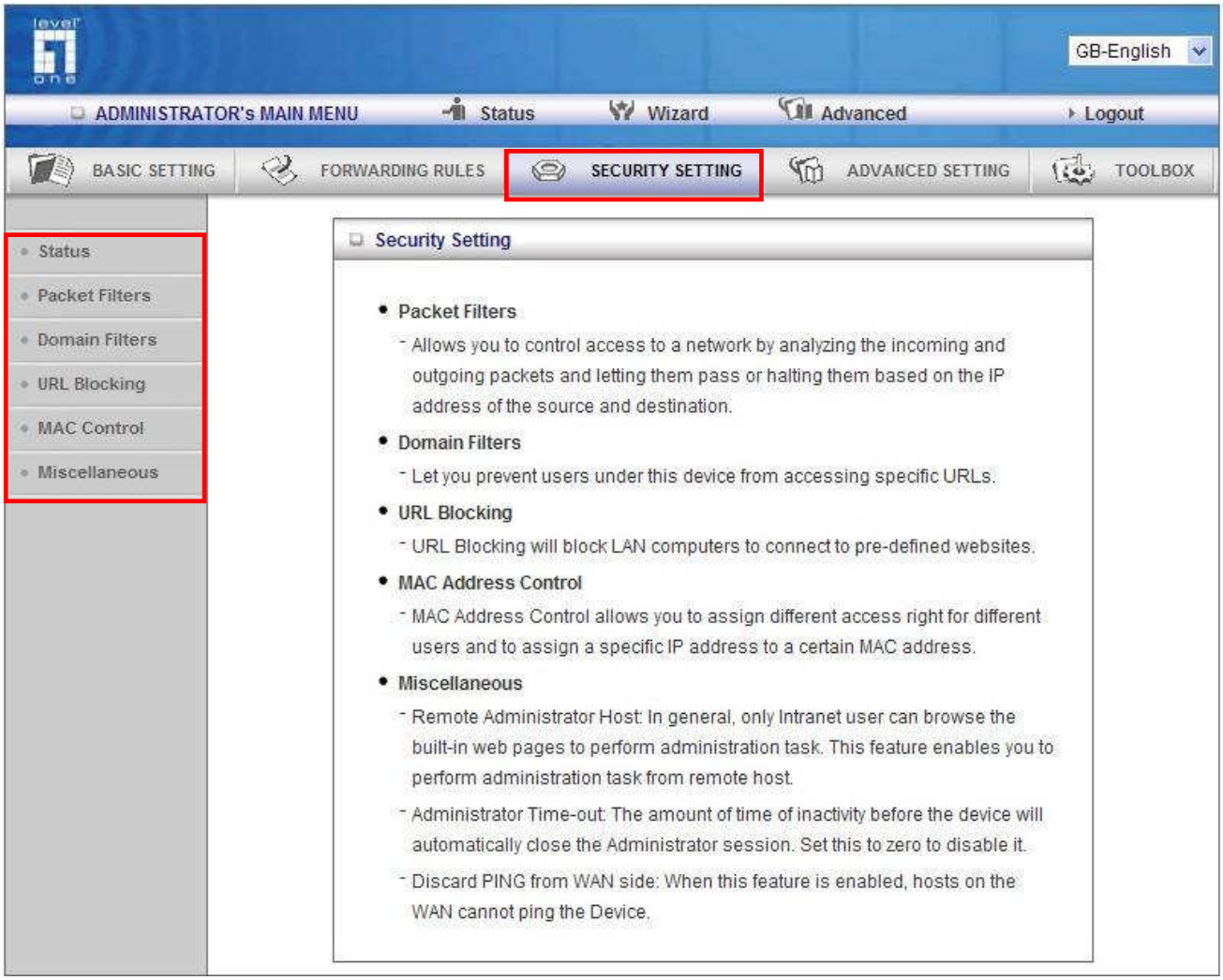

Internet Gateway Device UPnP
A new device is now available on your network. For more information, click here.
Crazy Browser...
(Untitled) - Et...
Address
My Network Places
Network Tasks
Add a network place
View network connections
Set up a home or small office network
Local Network
Internet Gateway Device UPnP
The Internet

Xbox Support

The Xbox is a video game console produced by Microsoft Corporation. Please enable this function when you play games.

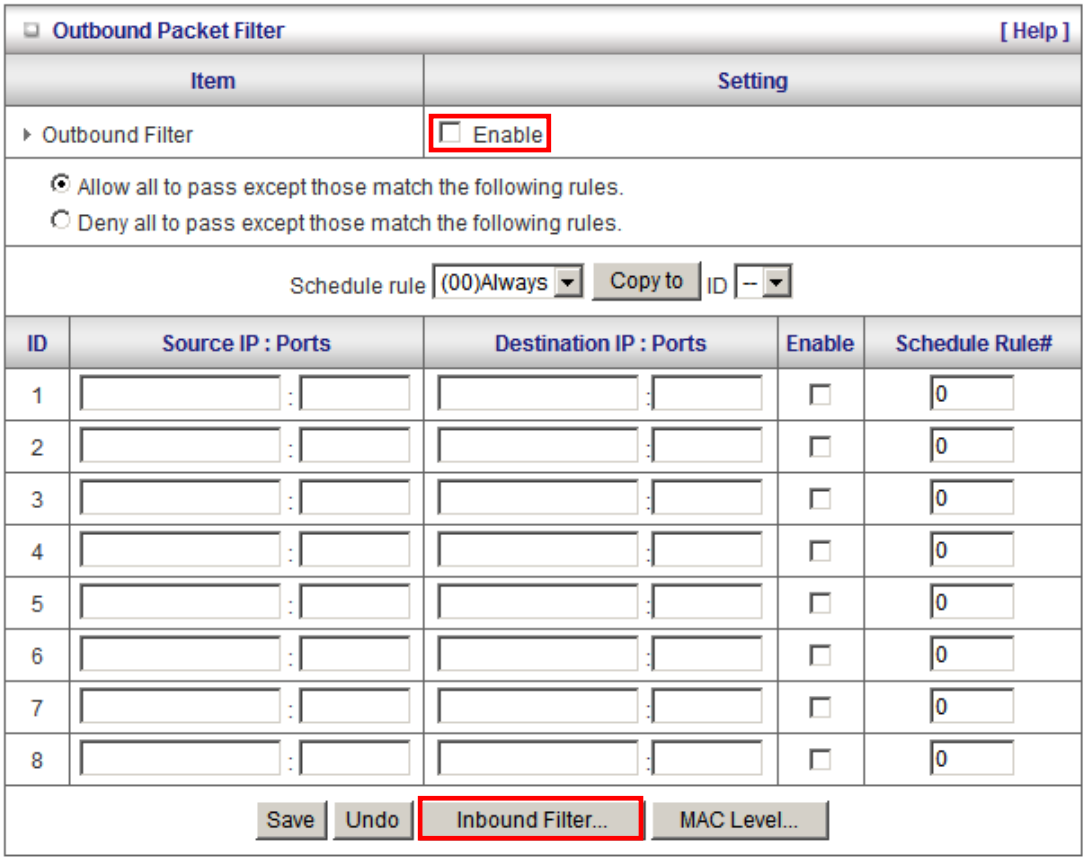
Security Settings

This section allows you to configure the security management of the unit. Click on the menu on the left to access the respective setting page.


GB-English
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
Status
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Security Setting
Packet Filters
- Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
Domain Filters
- Let you prevent users under this device from accessing specific URLs.
URL Blocking
- URL Blocking will block LAN computers to connect to pre-defined websites.
MAC Address Control
- MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
Miscellaneous
- Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
- Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
- Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

Packet Filter

Packet Filters allows you to control what packets are allowed to pass through the WBR-6603. The Outbound Filter applies to all outbound packets and the Inbound Filter only applies to packets that are destined to Virtual Servers or the DMZ Host only.



To enable the Outbound Filter, tick the **Enable** tick box.

There are two types of filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound.
For each rule, you can define the following:

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP or both.
- Use Schedule Rule#

For source or destination IP address, you can define a single IP address (192.168.1.1) or a range of IP addresses (192.168.1.100 – 192.168.1.200). An empty implies all IP addresses.

For source or destination port, you can define a single port (80) or a range of ports (1000-1999). You also need to add prefix "T" or "U" to specify TCP or UDP protocol, for example T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses.

Packet Filter can also work with Scheduling Rules and give users more flexibility on Access control. For more detail, please refer to Scheduling Rule (Advanced Setting > Schedule Rule).

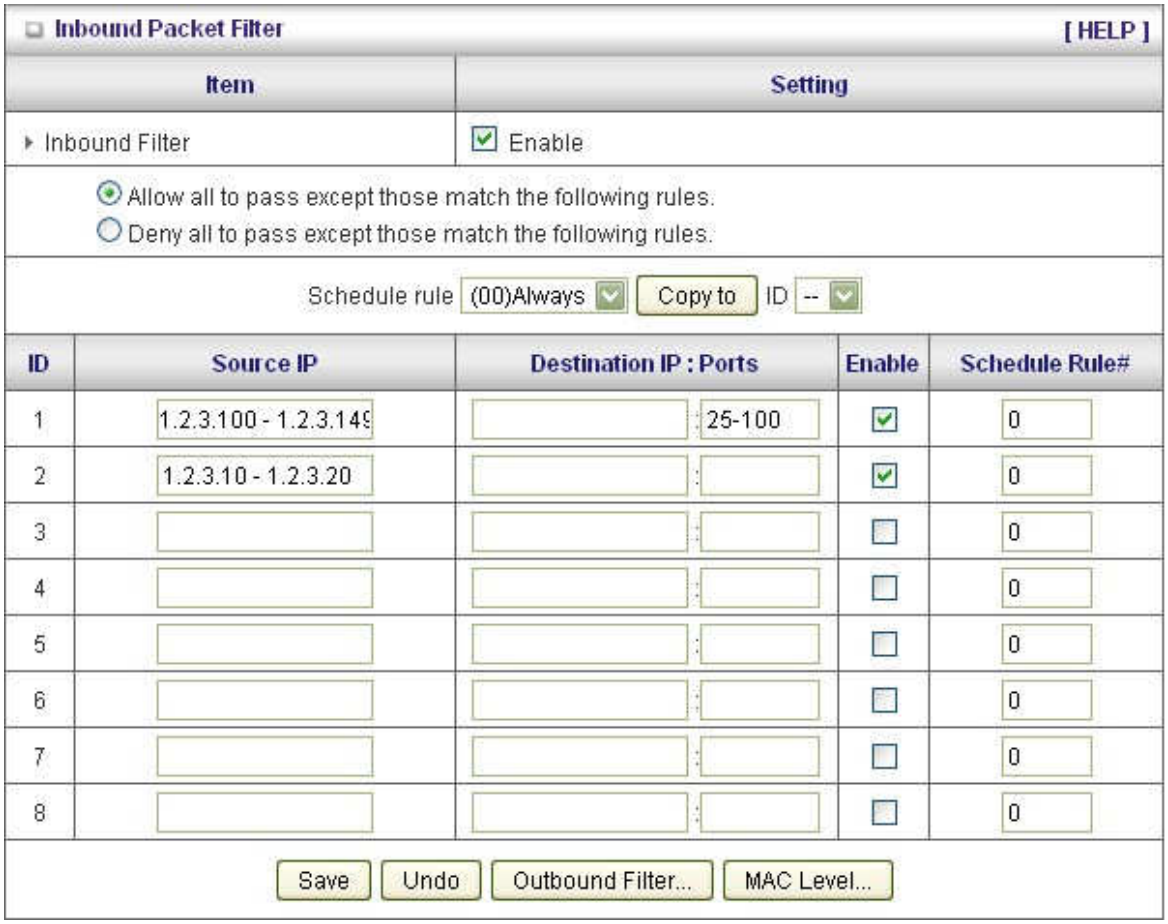
Each rule can be enabled or disabled individually.

Inbound Filter:

To access the Inbound Packet Filter page, click on **Inbound Filter** on the bottom of the page. All settings on this page are similar to Outbound Filters.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

Example 1:

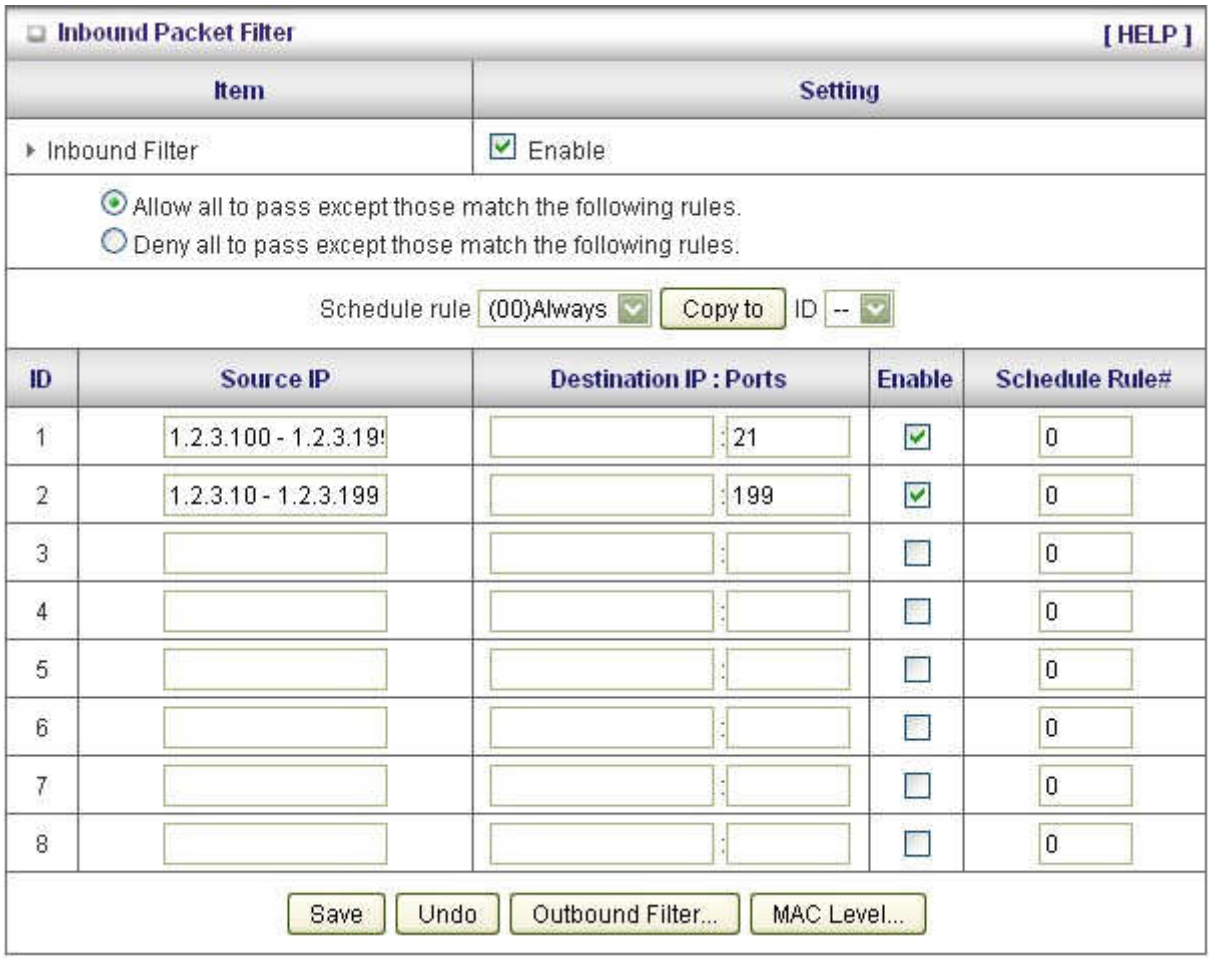


(1.2.3.100-1.2.3.149) Remote hosts are allow to send mail (port 25), and browse the Internet (port 80)

(1.2.3.10-1.2.3.20) Remote hosts can do everything (block nothing)

Others are all blocked.

Example 2:


Inbound Packet Filter [HELP]

Item	Setting
Inbound Filter	Enable

Allow all to pass except those match the following rules.
Deny all to pass except those match the following rules.

Schedule rule (00)Always Copy to ID --

ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	1.2.3.100 - 1.2.3.19	: 21	☑	0
2	1.2.3.10 - 1.2.3.199	: 199	☑	0
3		:	☐	0
4		:	☐	0
5		:	☐	0
6		:	☐	0
7		:	☐	0
8		:	☐	0

Save Undo Outbound Filter... MAC Level...

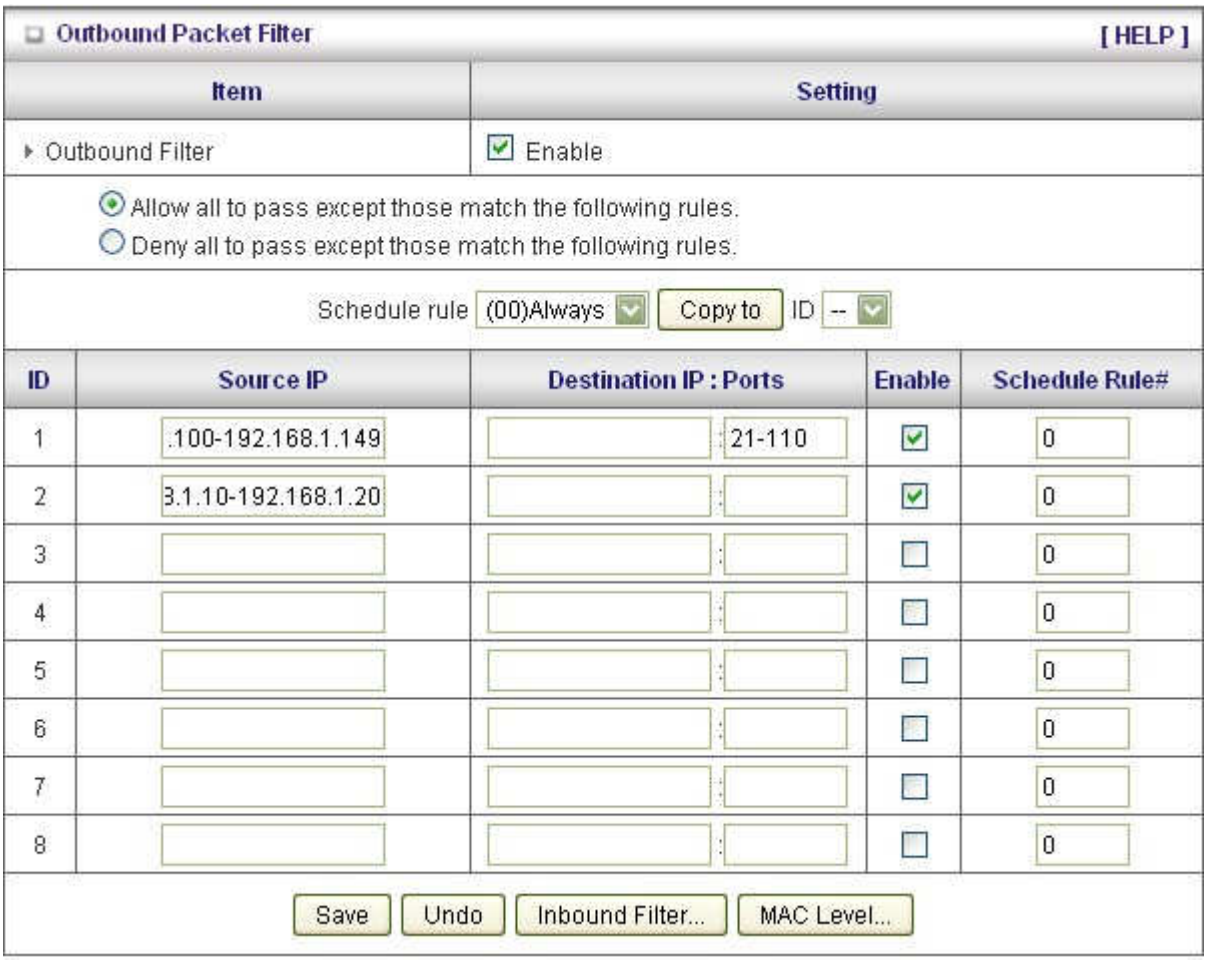
(1.2.3.100-1.2.3.199) Remote hosts can do everything except read net news (port 199) and transfer files via FTP (port 21) behind Router Server.
Others are all allowed.

After **Inbound Packet Filter** setting is configured, click the **save** button.

Outbound Filter:

To enable **Outbound Packet Filter** click the check box next to **Enable** in the **Outbound Packet Filter** field.

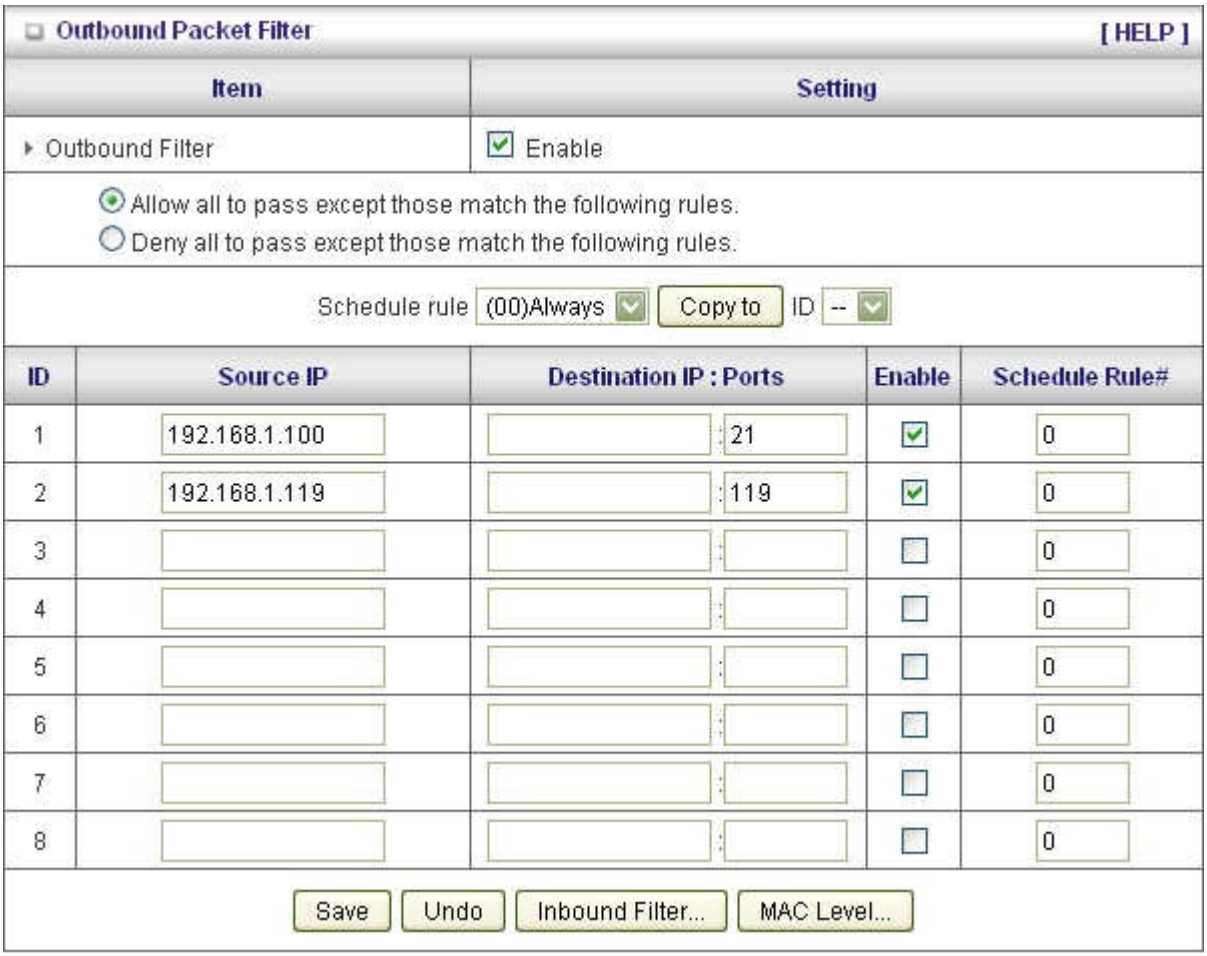
Example 1:



(192.168.1.100-192.168.1.149) Located hosts are only allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.1.10-192.168.1.20) Located hosts can do everything (block nothing)
Others are all blocked.

Example 2:



(192.168.1.100 and 192.168.1.119) Located Hosts can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed.

After **Outbound Packet Filter** setting is configured, click the **save** button.

Domain Filter

The Domain Filter enables you to prevent users from accessing specific domain addresses (web sites).

To enable Domain Filter, make sure to tick the **Enable** tick box.

- **Log DNS Query**: Check if you want to log the action when someone accesses the specific URLs.
- **Privilege IP Addresses Range:** Setting a range of hosts and privilege these hosts to access the internet without any restrictions.
- **Domain Suffix**: A suffix of URL to be restricted; For example, ".com", "xxx.com".
- **Action**: When someone is accessing the URL that meets the domain suffix, what kind of action you want the WBR-6603 to take. Tick on **Drop** to block the access and/or tick on **Log** to log the access.
- **Enable**: Tick to enable each rule.
- **Schedule Rules**: Please enter the Schedule rules # you want to apply. For further setting please see "**page 61**" **Schedule Rule**.

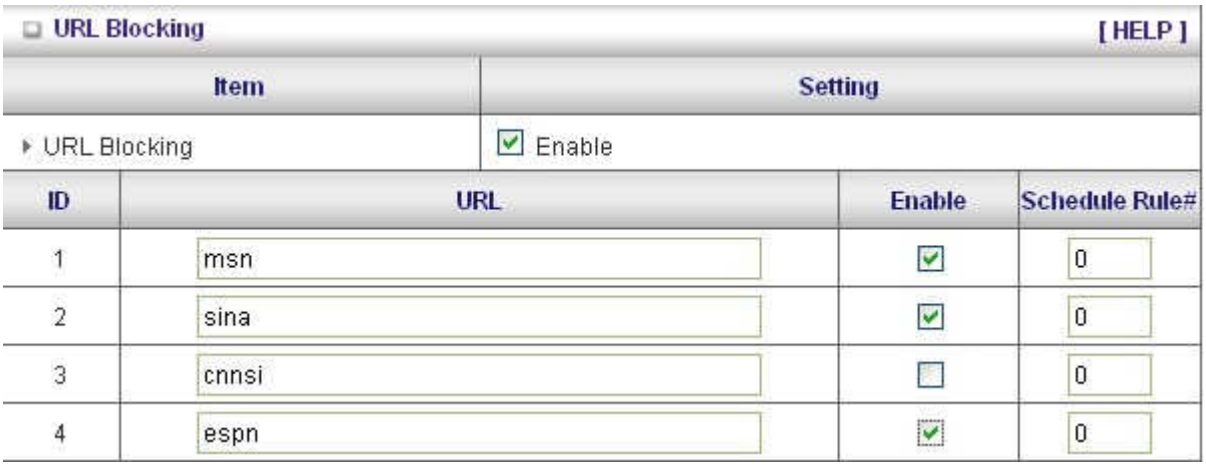
In this example:

1. URL include "www.msn.com" will be blocked, and the action will be record in log-file.
2. URL include "www.sina.com" will not be blocked, but the action will be record in log-file.
3. URL include "www.google.com" will be blocked, but the action will not be record in log-file.
4. IP address X.X.X.100~ X.X.X.199 can access network without restriction.

URL Blocking

URL Blocking will block LAN computers from connecting to a pre-defined Web Site. The major difference between Domain Filter and URL Blocking is that Domain Filter requires the user to input suffixes (etc: xxx.com, ttt.net) while URL Blocking only requires user to input a keyword.

In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.



To enable URL Blocking, make sure to tick **Enable.**

To set an URL Blocking rule, you will require:

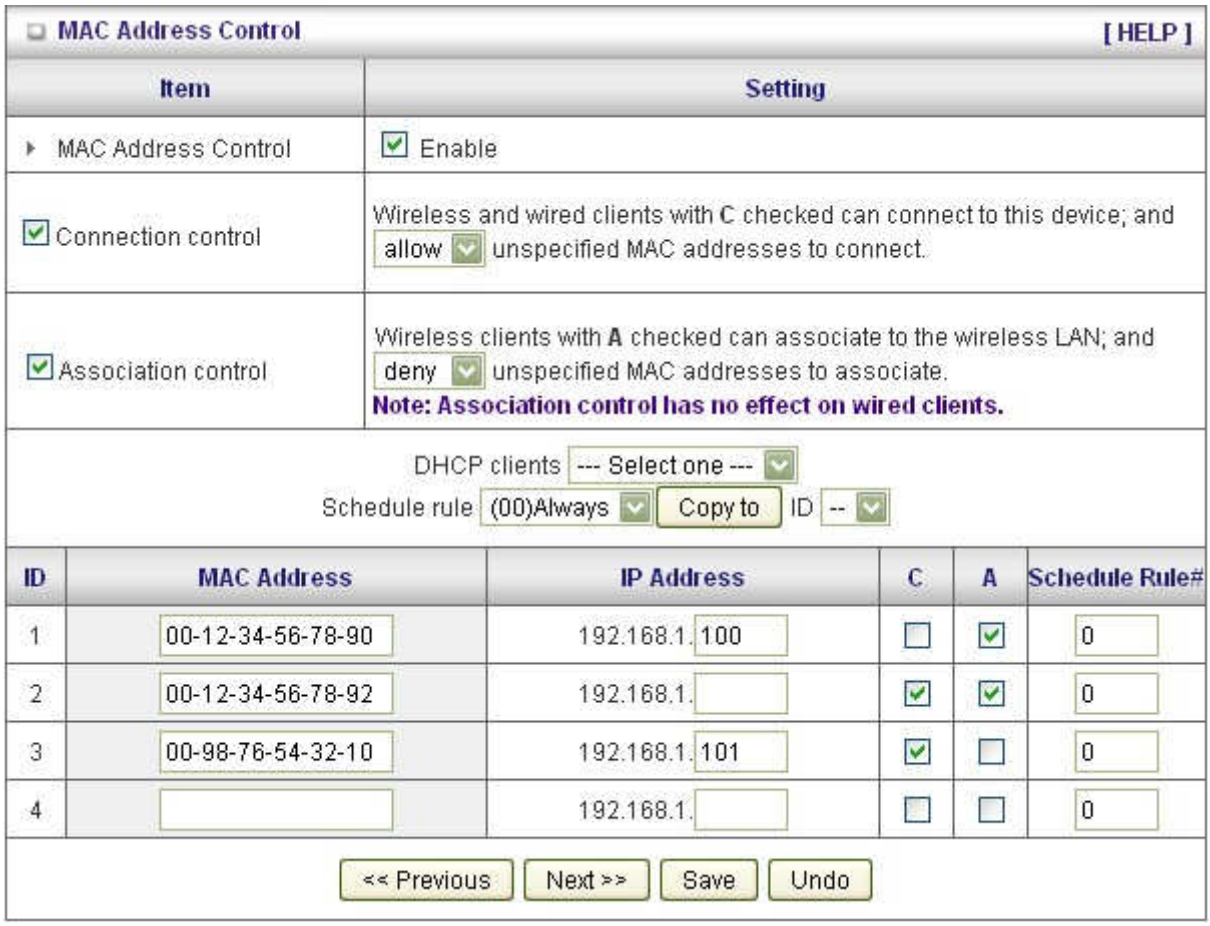
- **URL:** If any part of the Website's URL matches the predefined word, the connection will be blocked.
- **Enable**: Tick to enable the rule.
- **Schedule Rules**: Please enter the Schedule rules # you want to apply. For further setting please see “**page 61**” **Schedule Rule**.

In this example:

1. URL include “msn” will be blocked, and the action will be record in log-file.
2. URL include “sina” will be blocked, and the action will be record in log-file
3. URL include “cnnsi” will not be blocked, but the action will be record in log-file.
4. URL include “espn” will be blocked, and the action will be record in log-file

MAC Control

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.



To enable MAC Address Control, make sure to tick on **Enable.**
All of the settings in this page will take effect only when "**Enable**" is checked.

There are two types of control method available:

- **Connection Control:** To control which wired and wireless clients can connect to this device. If a client is denied access, it means the client cannot access the Internet either. Choose "allow" or "deny" to allow or deny the clients whose MAC addresses are not in the list.
- **Association Control:** To control which wireless client can be associated with this device. If a client is denied, then it means the client cannot send or receive any data via this WBR-6603. Choose "allow" or "deny" to allow or deny the clients with MAC addresses that are not in the list to associate to the wireless network.

MAC Address	MAC address indicates a specific client.
IP Address	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
C	When "**Connection control**" is checked, check "**C**" will allow the corresponding client to connect to this device.
A	When "**Association control**" is checked, check "**A**" will allow the corresponding client to associate to the wireless LAN.

In this page, we provide the following Combo box and button to help you to input the MAC address.

You can select a specific client in the DHCP clients Combo box, and then click on the “Copy to” button to copy the MAC address of the client you select to the ID selected in the “ID” Combo box.

Previous and Next Page

To make this setup page simple and clear, we have divided the “Control Table” into several pages. You can use these buttons to switch to different pages.

Example:

In this scenario, there are three clients listed in the Table. Clients 1 and 2 are wireless, and client 3 is wired.

1. The MAC Address Control" function is enabled.
2. **Connection Control** is enabled and all the wired and wireless clients not listed in the Control table are "Allowed" to connect to this device.
3. **Association Control** is enabled, and all of the wireless clients not listed in the Control table are "Denied" to associate to the wireless LAN.
4. Clients 1 and 3 have fixed IP address either from the DHCP server of this device or manually assigned:

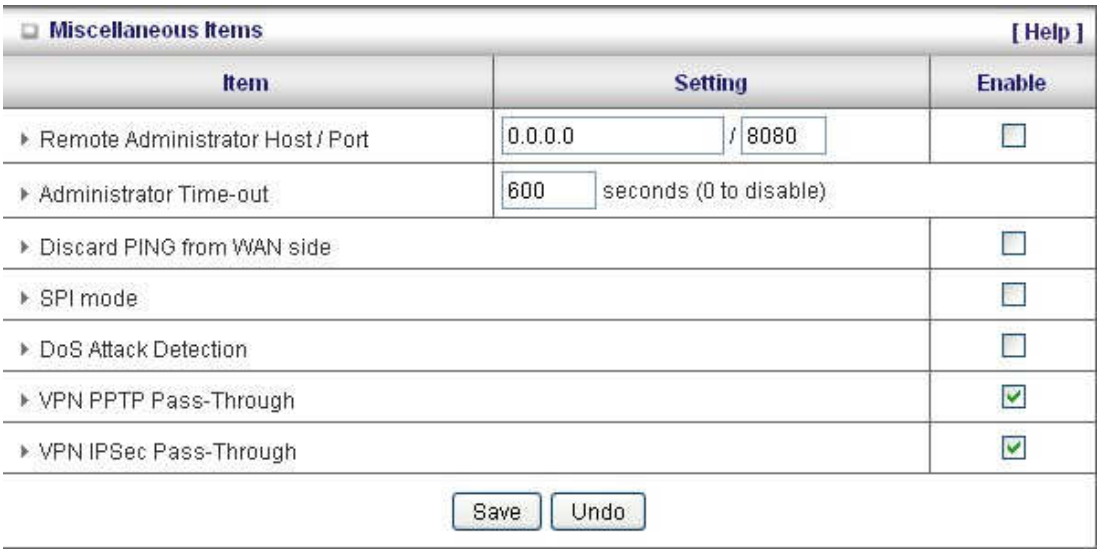
   ID 1 - "00-12-34-56-78-90" --> 192.168.1.100
   ID 3 - "00-98-76-54-32-10" --> 192.168.1.101

   Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.

   For example, Client 1 tries to use an IP address different from the address listed in the Control Table (192.168.1.100), it will be denied to connect to this device.
5. Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.
6. Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is not affected by Association control.

Miscellaneous

This page allows you to change various miscellaneous security settings.



Remote Administrator Host/Port: In general, only intranet user can browse the built-in web configuration pages to perform administration task. This feature enables you to perform administration task from the Internet. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task.

For better security, you can specify just one IP address or use subnet mask bits “/nn” notation to specify a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 8080. You can change web server port to other port.

Administrator Timeout: The amount of time with no activity before the user will be logged out of the web configuration pages. Set to zero to disable this feature.

Discard PING from WAN side: When enabled, any host on the internet cannot ping this device’s from WAN side.

SPI Mode: When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

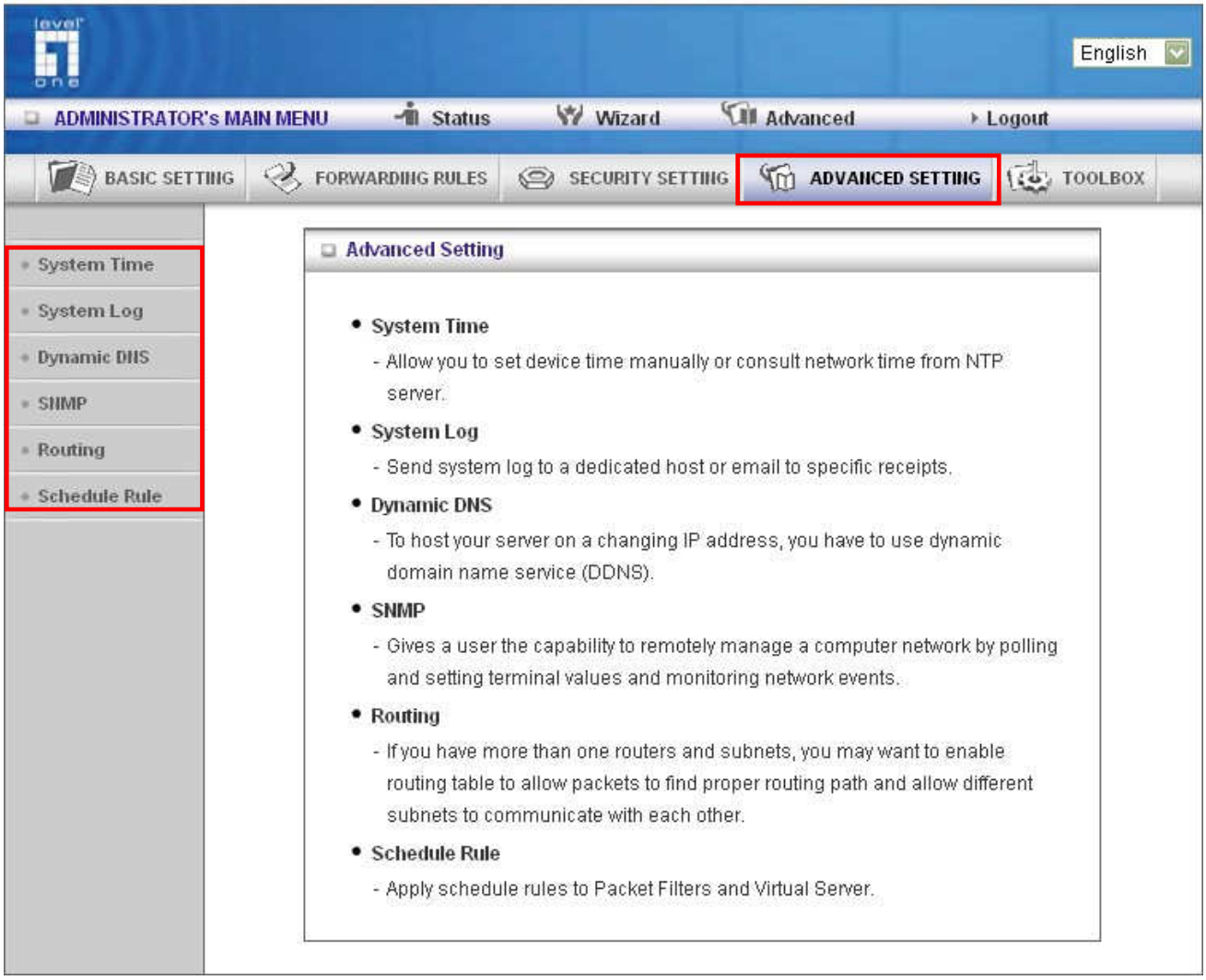
DoS Attack Detection: When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

VPN PPTP and IPSec Pass-Through:

Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the router supports IPSec Pass-through and PPTP Pass-through.

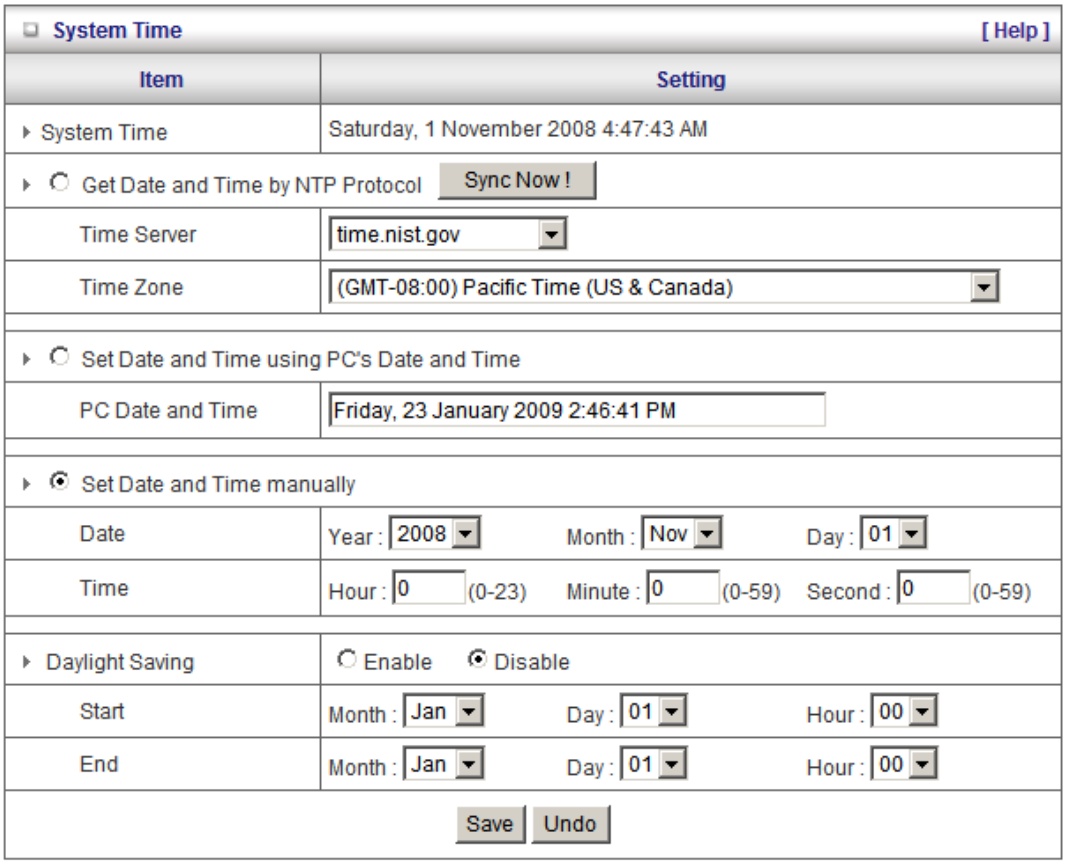
Advanced Settings

These pages allow you to configure the more advanced settings on the unit.


English
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Advanced Setting
System Time
- Allow you to set device time manually or consult network time from NTP server.
System Log
- Send system log to a dedicated host or email to specific receipts.
Dynamic DNS
- To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
SNMP
- Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
Routing
- If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
Schedule Rule
- Apply schedule rules to Packet Filters and Virtual Server.

System Time

This page allows you to set the time settings of the WBR-6603.



There are three ways to set up the System Time of the WBR-6603.

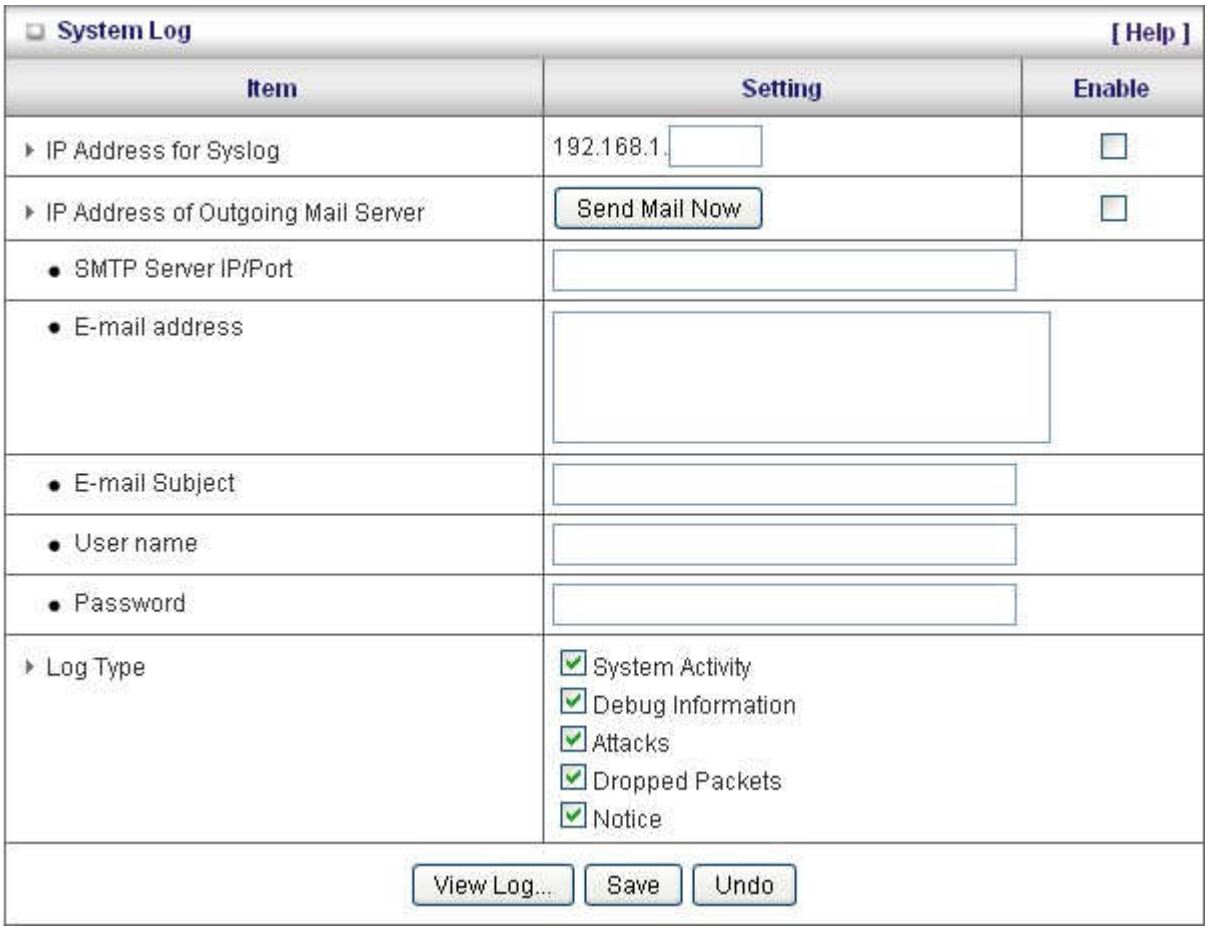
1. **Get Date and Time by NTP Protocol:** Selected if you want to get the Date and Time from an NTP server. A Time Server and time zone is required. Once entered, click **Sync Now** to sync the time with the Time Server.
2. **Set Date and Time using PC's Date and Time:** Set the Date and Time using the settings from your computer.
3. **Set Date and Time manually:** Selected if you want to Set Date and Time manually.

Daylight Saving:

If required, set the Daylight Saving settings by selecting Enable and define the Start and End dates for daylight savings periods.

System Log

The WBR-6603 supports both Syslog (using UDP packets) and E-Mail alert.



It support two methods to export system logs to specific destination by means of syslog (UDP) and E-mail (TCP). The items you have to setup including:

Syslog setting:

For Syslog, you will need to enter the IP address of the host computer that will be receiving the syslog messages and tick on **Enable**.

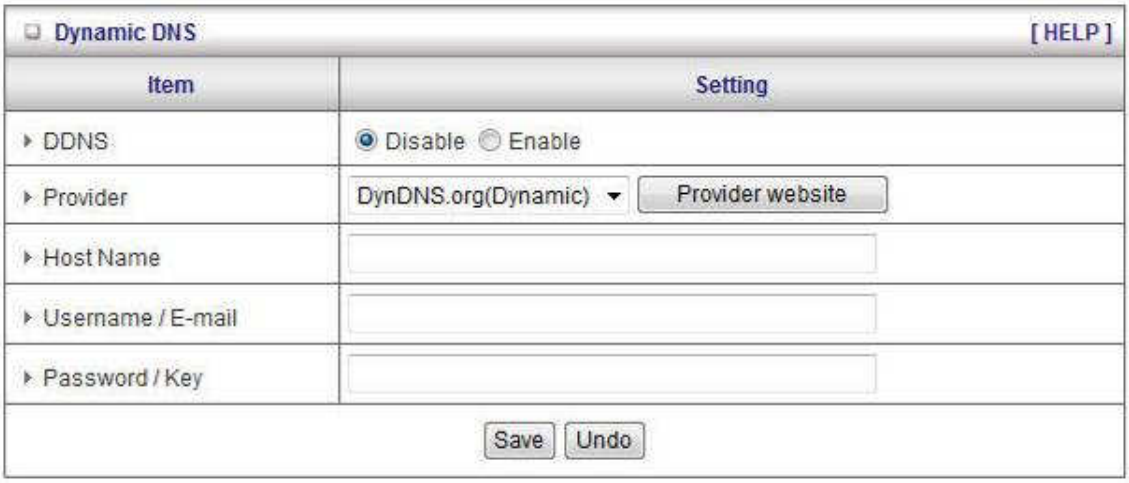
E-mail alert:

For E-Mail alert, you will need to define the following:

- **E-Mail Alert:** Tick **Enable** to enable this feature.
- **SMTP Server IP and Port:** Enter the IP address and port of the SMTP server, separated by ":" (no quotes). If you do not specify the port number, the default value of 25 will be used.
- **E-Mail addresses:** Enter the e-mail addresses of the recipients for the email logs. To assign more than one recipient, use ";" or "," (no quotes) to separate the e-mail addresses.
- **E-Mail Subject:** Enter the subject for the e-mail (optional)
- **User Name / Password:** Username and Password if your SMTP server requires log in.

Dynamic DNS

Dynamic DNS is a feature that allows users to set up a static domain name even when they have a dynamic internet IP address. So even if your IP address changes every time you connect to your ISP, the IP address can be mapped to a host name so that anyone who wants to connect to the WBR-6603, or any services behind the router from the internet can just use the Dynamic DNS hostname instead of the IP address which might change.



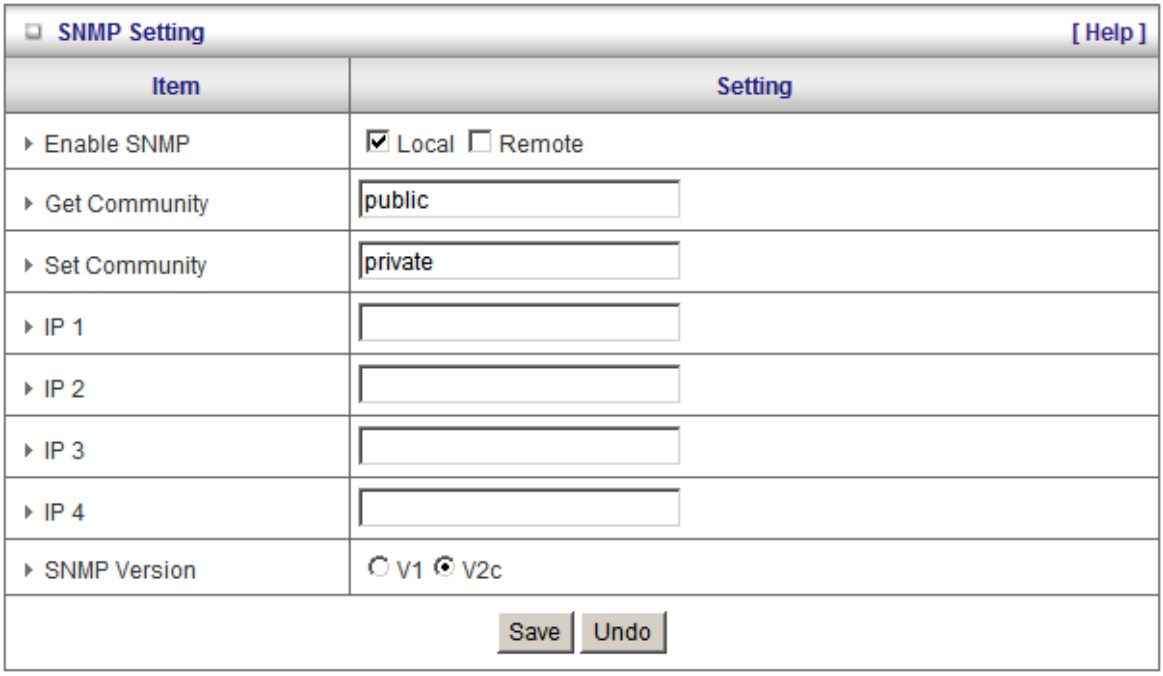
Before you enable **Dynamic DNS**, you need to register an account on one of the supported Dynamic DNS providers in the list. After successfully registering the account, the Dynamic DNS provider would provide you with the following details:

- Host Name
- Username/Email
- Password

To enable Dynamic DNS click the check box next to Enable in the DDNS field and choose the respective Dynamic DNS provider. Enter the required details and then click **Save** to save the settings or **Undo** to cancel.

SNMP Setting

SNMP (Simple Network Management Protocol) is designed to give users the ability to remotely manage a computer or network device.



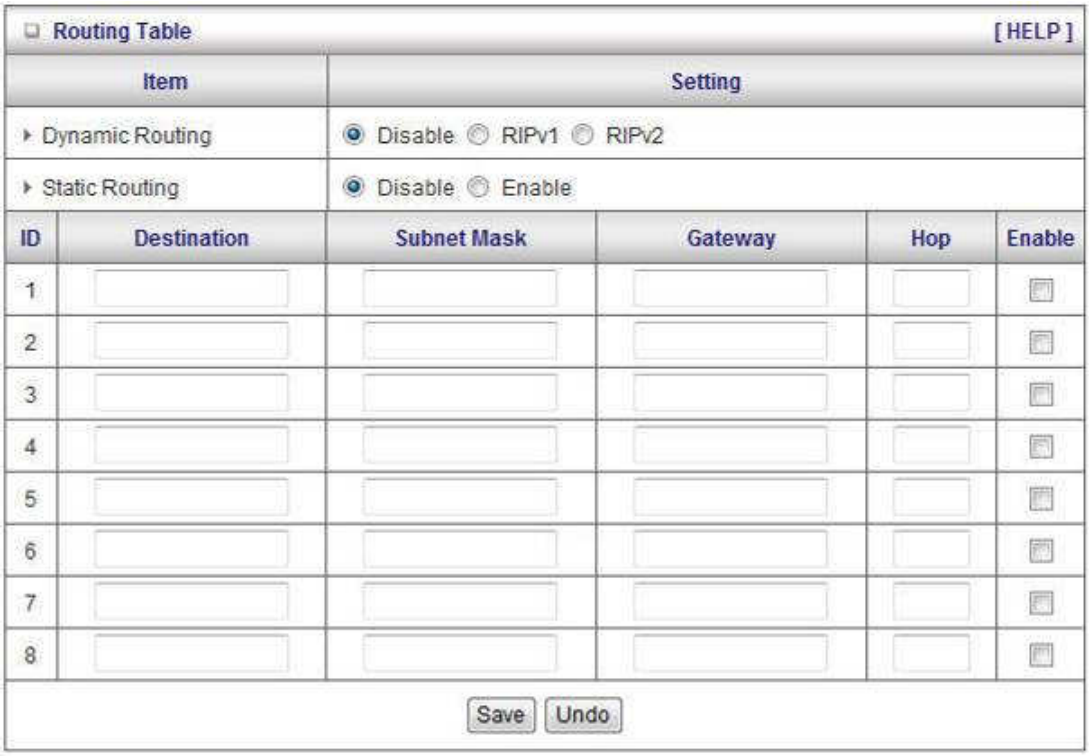
To enable SNMP, please set the following:

- **Enable SNMP:** You must check either Local or Remote or both to enable SNMP function. If Local is checked, this unit will respond to requests from LAN. If Remote is checked, the unit will respond to requests from WAN.
- **Get Community:** Set the community of public. This will act as a password.
- **Set Community:** Set the community of private. This will act as a password.
- **IP 1,IP 2,IP 3,IP 4:** Enter the IP addresses of the managed PCs. The unit will send SNMP Trap messages only to the IP addresses listed.
- **SNMP Version:** Please select the SNMP Version of your SNMP Management software.

Click on **Save** to save the settings or **Undo** to cancel.

Routing

When you have more than one WBR-6603, or router with different subnets on the network, you will need to enable this function to allow the different subnets to communicate with each other.



There are two types of routing supported by the WBR-6603.

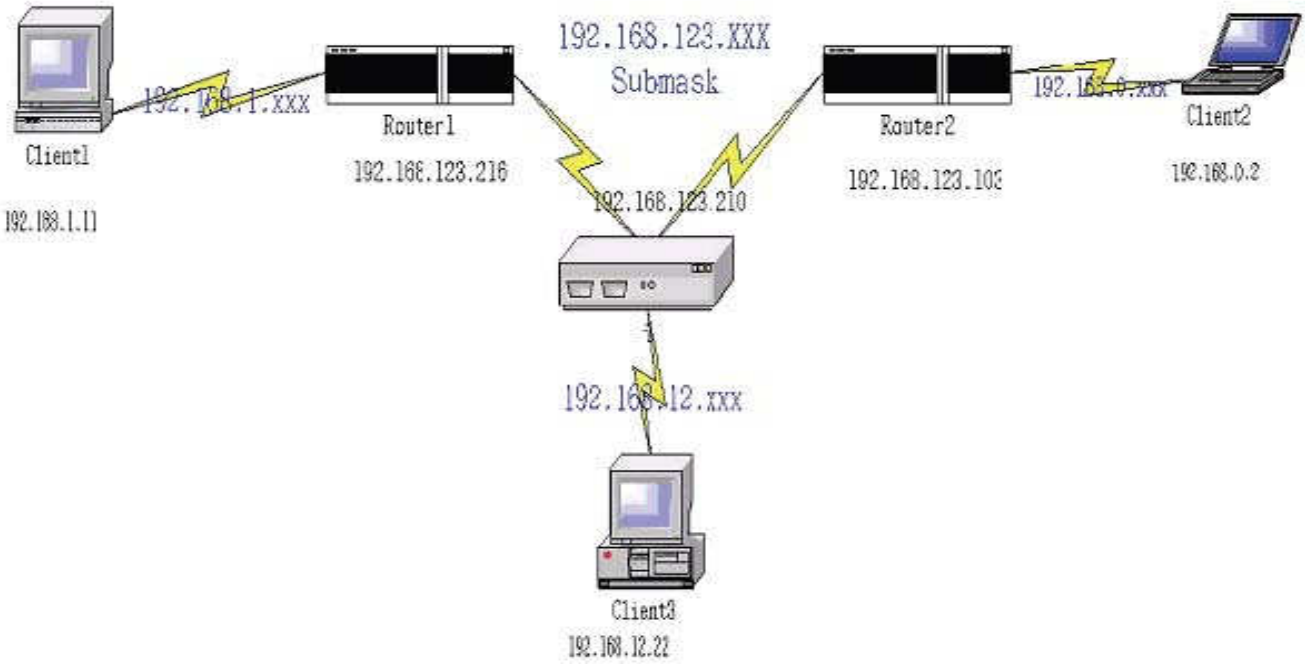
- **Dynamic Routing:** This method uses Routing Information Protocol (RIP) to enable the devices to determine the best route for each packet based on the number of hops between the source and destination.

  Tick the **Enable** box to enable Dynamic Routing. Use RIPv2 only if you have different subnets in your network. Otherwise, please select RIPv1 if you need this protocol.

- **Static Routing:** Allows computers that are connected to the WBR-6603 to communicate with computers on other LAN segments which are connected to the WBR-6603 using a different router. You can specify up to eight routing rules.

  The details below are required to set the routing rules:

  - IP Address
  - Subnet Mask
  - Gateway
  - Hop, number of hops
  - Tick **Enable** for each rule.



Destination	Subnet Mask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	✓
192.168.0.0	255.255.255.0	192.168.123.103	1	✓

So if, for example, Client3 wants to send an IP data packet to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (Router 2)

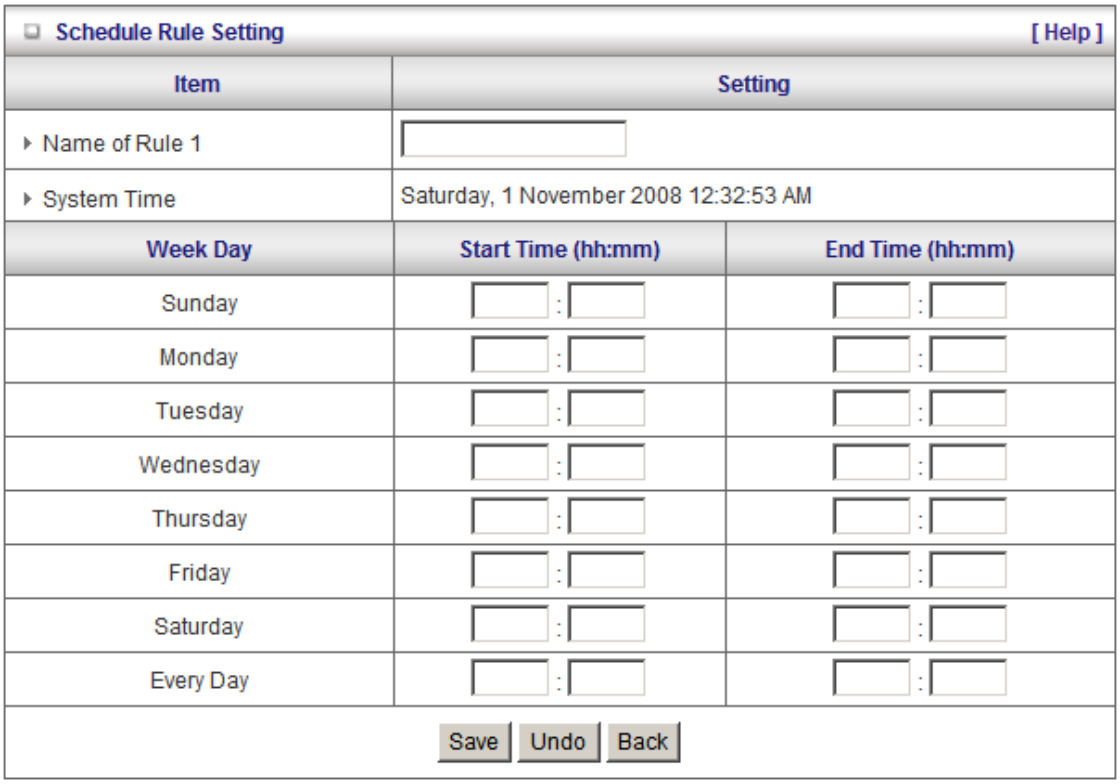
And if it sends Packets to 192.168.1.11 will go via 192.168.123.216 (Router 1)
Each rule can be enabled or disabled individually.

After **routing table** setting is configured, click the **save** button.

Schedule Rule

This feature allows you to define the time schedule of Virtual Server and Packet Filter rules.

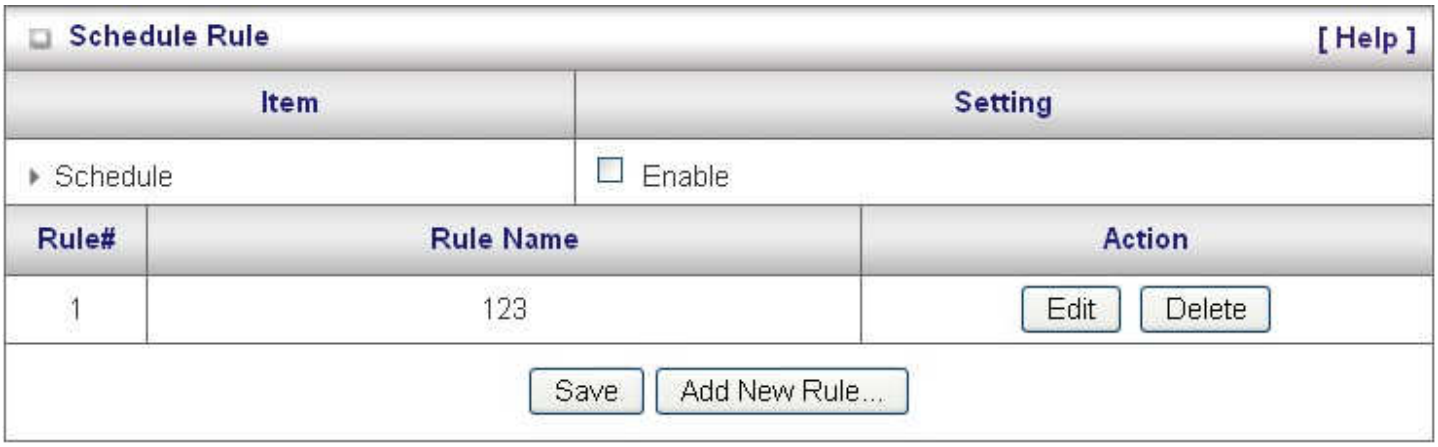
To enable Scheduling, tick **Enable** and click **Save**.
Then create new rules by pressing the **Add New Rule** button.



Enter the Rule's Name and set the Start and End Times for each day. Then click **Save** to save the new rule.

Once defined, you can use it for Wireless setting, Virtual Server, Packet/Domain Filters, and URL Blocking by entering the rule number in the "Schedule Rule#" fields.

When you set up the schedule rule, it will have rules in rule table as following:



Schedule Enable

Selected if you want to enable the Schedule.

Edit

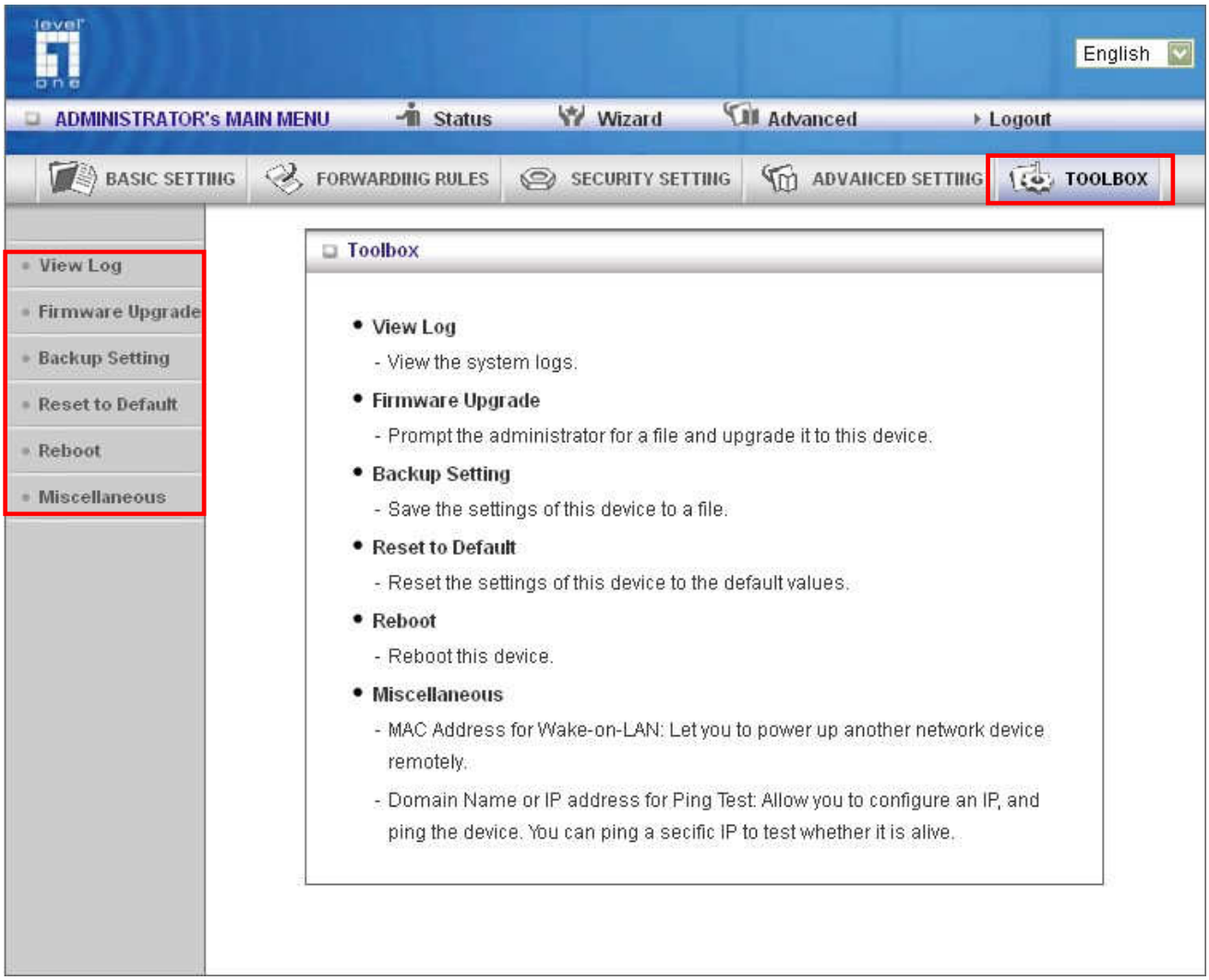
To edit the schedule rule.

Delete

To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

Toolbox

This section has some basic tools to maintain the WBR-6603 systems.


English
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX
View Log
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous
Toolbox
View Log
- View the system logs.
Firmware Upgrade
- Prompt the administrator for a file and upgrade it to this device.
Backup Setting
- Save the settings of this device to a file.
Reset to Default
- Reset the settings of this device to the default values.
Reboot
- Reboot this device.
Miscellaneous
- MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
- Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a secific IP to test whether it is alive.

View Log

You can View system log by clicking the View Log button.

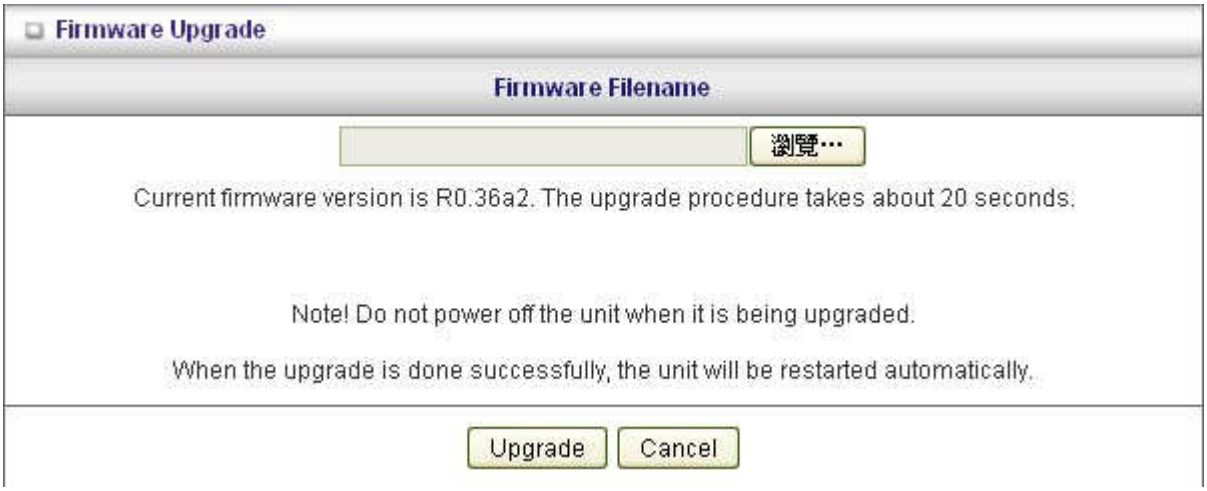
System Log

Item	Info
WAN Type:	Dynamic IP Address (R0.03b1)
Display time	Sat Nov 01 00:43:33 2008

Time	Log
Saturday, 1 November 2008 12:01:32 AM	Associated: 00-1F-1F-1F-6E-D4 st=0
Saturday, 1 November 2008 12:01:41 AM	DOD:triggered internally
Saturday, 1 November 2008 12:01:41 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:01:51 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:02:05 AM	Admin from 192.168.0.101 login successfully
Saturday, 1 November 2008 12:02:11 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:02:51 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:04:13 AM	DOD:triggered internally
Saturday, 1 November 2008 12:04:13 AM	DHCP:discover(My Host)
Saturday, 1 November 2008 12:04:23 AM	DHCP:discover(My Host)

Firmware Upgrade

This page allows you to perform updates to the firmware of the WBR-6603.

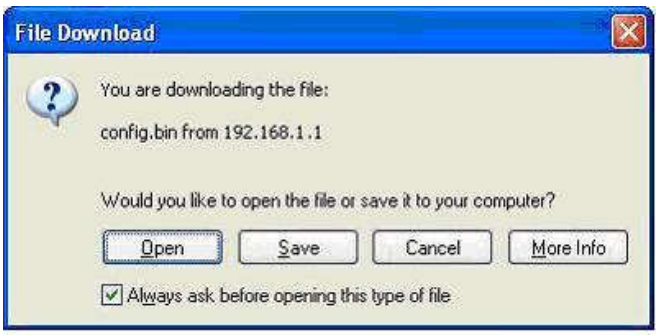

Firmware Upgrade
Firmware Filename
瀏覽...
Current firmware version is R0.36a2. The upgrade procedure takes about 20 seconds.
Note! Do not power off the unit when it is being upgraded.
When the upgrade is done successfully, the unit will be restarted automatically.
Upgrade
Cancel

To use, click **Browse** and locate the firmware image file, then click **Upgrade**.

Note: Please connect to the WBR-6603 using a wired LAN connection as if the connection breaks during the update, it will render the unit unworkable. Also disable any anti-virus or firewall program before beginning the update.

Backup Setting

You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.


File Download
You are downloading the file:
config.bin from 192.168.1.1
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

Reset to Default

You can also reset the unit back to factory default settings by clicking the **Reset to Default** button and click OK. Please reboot the device to make the settings effect.

Reboot

To reboot the unit manually, click the **Reboot** button and click OK.

Miscellaneous

MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

Domain Name or IP Address for Test

Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Appendix A 802.1x Setting

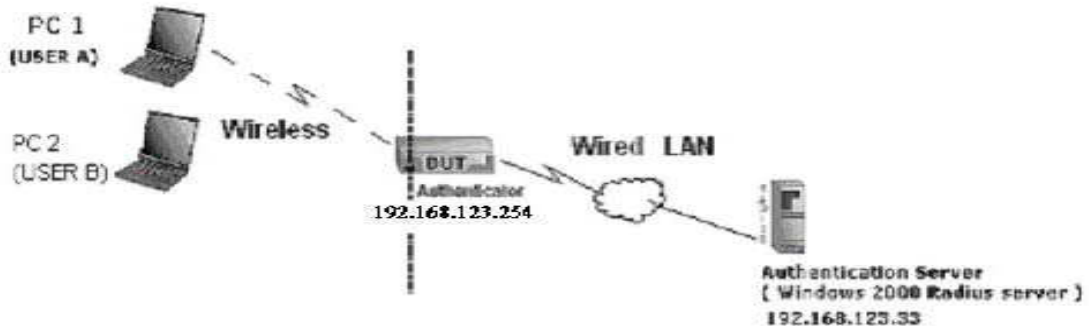


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

Equipment Details

PC1: Microsoft Windows XP Professional without Service Pack 1 and LevelOne Wireless PCI Card

PC2: Microsoft Windows XP Professional with Service Pack 1a or later and LevelOne Wireless PCI Card.

Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.

Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and HotFix Q313664 *(You can get more information from http://support.microsoft.com/default.aspx?scid=kb; en-us;313664)*

DUT Configuration:

1. Enable DHCP server.
2. WAN setting: static IP address.
3. LAN IP address: 192.168.123.254/24.
4. Set RADIUS server IP.
5. Set RADIUS server shared key.
6. Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP_TLS, PEAP_CHAPv2(Windows XP with SP1 only), and PEAP_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

DUT and Windows 2000 Radius Server Setup

Setup Windows 2000 RADIUS Server

We have to change authentication method to MD5_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

Setup DUT

1. Enable the 802.1X (check the “Enable checkbox“).
2. Enter the RADIUS server IP.
3. Enter the shared key. (The key shared by the RADIUS server and DUT).
4. We will change 802.1X encryption key length to fit the variable test condition.

Setup Network adapter on PC

1. Choose the IEEE802.1X as the authentication method. (Fig 2)
2. Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.
3. If choosing use smart card or the certificate as the EAP type, we select to use a certificate on this computer.
4. We will change EAP type to fit the variable test condition.

Figure 2 is a setting picture of Windows XP without service pack 1. If users upgrade to service pack 1, then they can’t see MD5-Challenge from EAP type list any more, but they will get a new Protected EAP (PEAP) option.

Wireless Network Connection Properties
General
Wireless Networks
Authentication
Advanced
Select this option to provide authenticated network access for wired and wireless Ethernet networks.
Enable network access control using IEEE 802.1X
EAP type:
Smart Card or other Certificate
MD5-Challenge
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

Figure 2: Enable IEEE 802.1X access control / Smart card or certificate properties

Windows 2000 RADIUS server Authentication testing:

DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

1. Download and install the certificate on PC1. (Fig 4)
2. PC1 chooses the SSID of DUT as the Access Point.
3. Set authentication type of wireless client and RADIUS server both to EAP_TLS.
4. Disable the wireless connection and enable again.
5. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC1. (Fig 5)
6. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. (Fig 6)
7. Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.

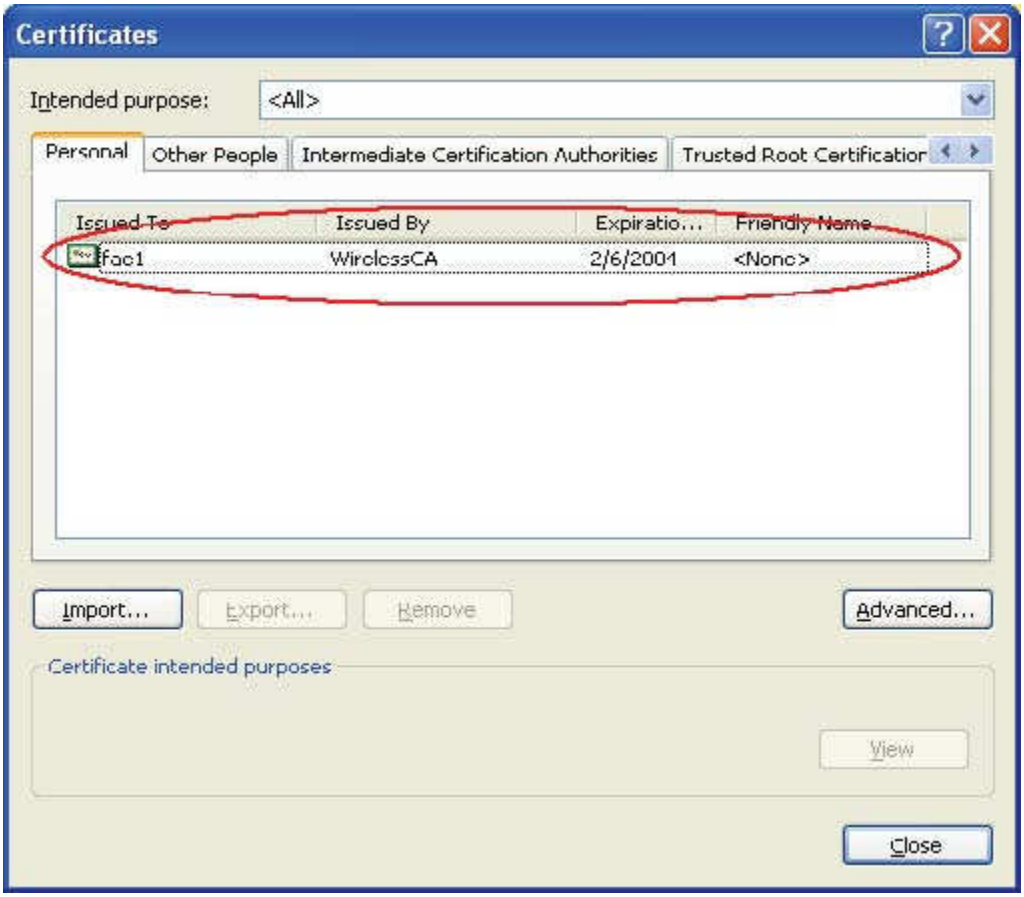


Figure 4: Certificate information on PC1

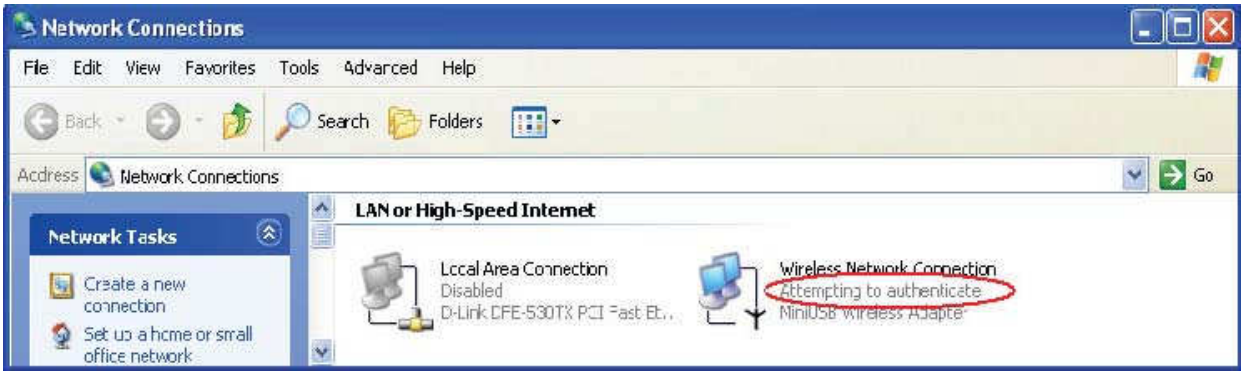


Figure 5: Authenticating

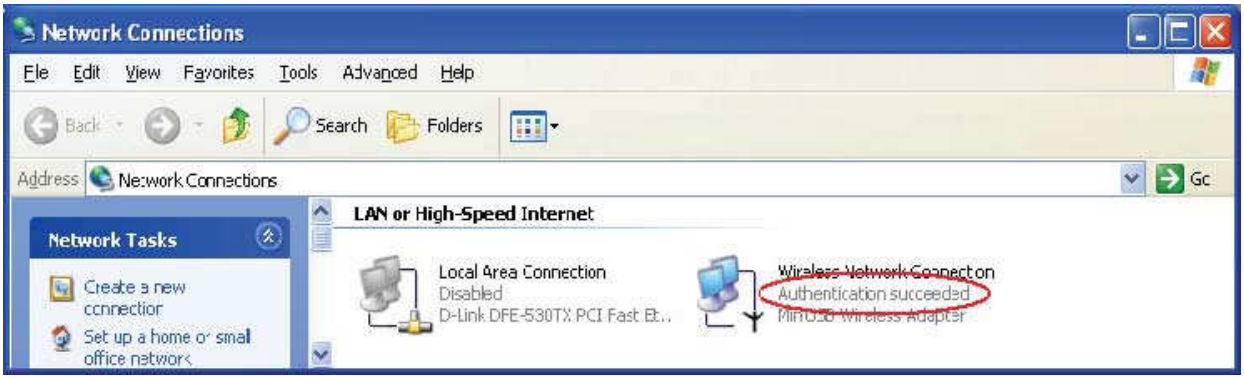


Figure 6: Authentication success

DUT authenticate PC2 using PEAP-TLS.

1. PC2 chooses the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP_TLS.
3. Disable the wireless connection and enable again.
4. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC2.
5. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.
6. Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

Support Type: The router supports the types of 802.1x Authentication: PEAP-CHAPv2 and PEAP-TLS.

Appendix B FAQ and Troubleshooting

This chapter covers some common problems that may be encountered while using the Wireless ADSL Router and some possible solutions to them. If you follow the suggested steps and the Wireless ADSL Router still does not function properly, contact your dealer for further advice.

What can I do when I have some trouble at the first time?

1. Why can't I connect to the Wireless ADSL Router to configure it?

A: Check the following:

- The Wireless ADSL Router is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Wireless ADSL Router are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.2 to 192.168.1.254 and thus com-patible with the Wireless ADSL Router's default IP Address of 192.168.0.1. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless ADSL Router. In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

2. Why can't I connect the router even if the cable is plugged in LAN port and the LED is light?

A: First, please check Status LED. If the device is normal, the LED will blink once per second.
If not, please check the blinking Status LED as shown:

Status LED stays constantly on or off:
The system is frozen. Suggest powering off and on the router. If this symptom continues to occur, please reset to default settings or upgrade to the latest firmware and try again.

Status LED flashes irregularly: There is an error in the system. Please reset to default settings and reboot the router.

3. How to reset to factory default?

A: You can Restore the device by pressing "Wireless on/off" and "WPS" button.
Please make sure the ADSL router is power on and ready to use. Press the Wireless on/off button and WPS button simultaneously, keep the buttons pressed until 5 seconds, and then release. If the Status LED flashes about 5 times, the RESTORE process is completed.

4. When I connect to internet, some applications do not run properly when using the Wireless ADSL router.

A: The Wireless ADSL Router processes the data passing through it, so it is not transparent.
For incoming connections, you must use the Virtual Server or Firewall Rules to specify the PC which will receive the incoming traffic.
You can also use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one PC can use this feature.

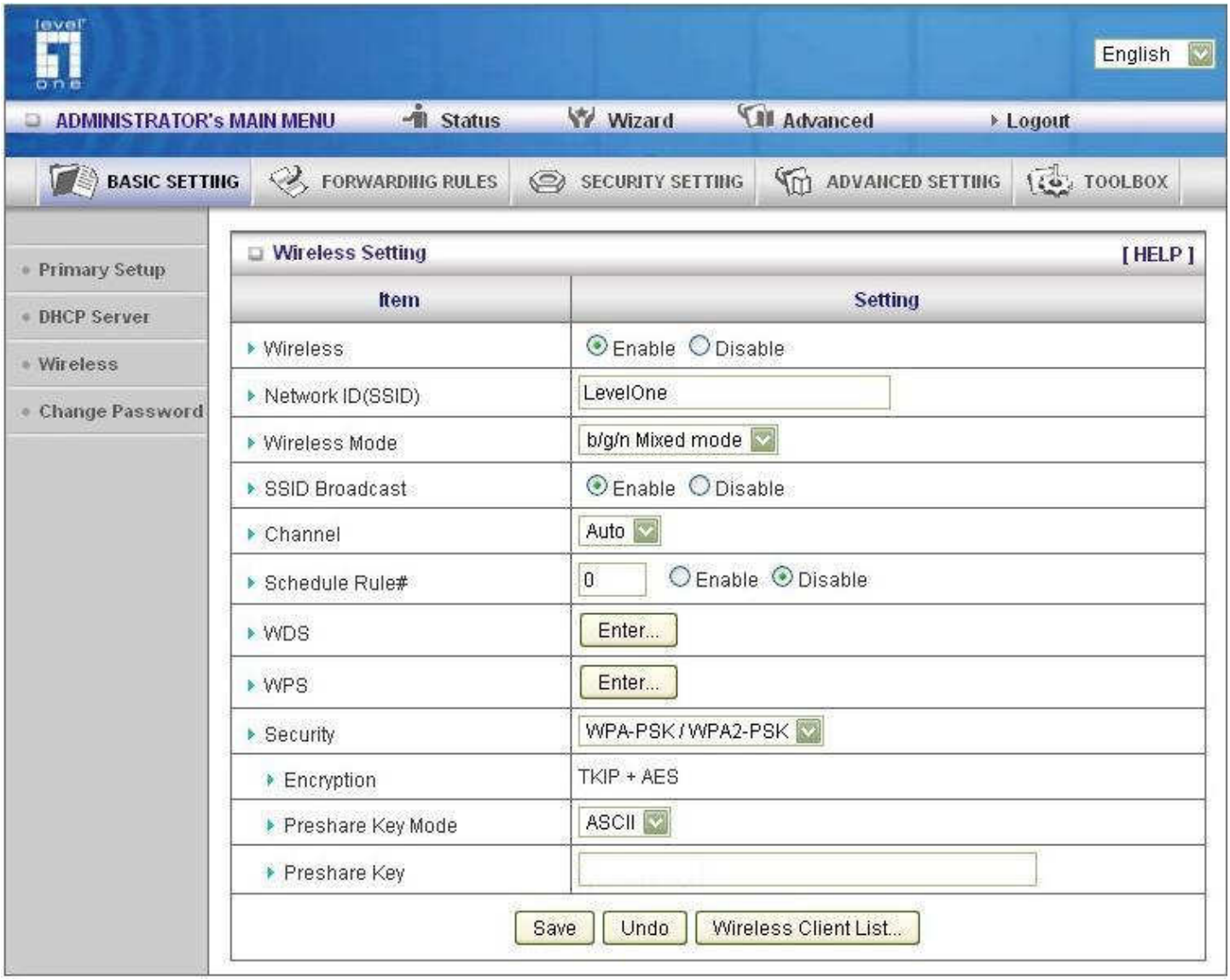
5. **When I use Static IP Address to connect to the Internet, I can access or ping global IP addresses such as 202.93.91.218. However, I cannot access the website by using its domain name, for example http://espn.com ?**

A: Please check the DNS configuration of Static IP Address. Please refer to the information of ISP and assign one or two DNS servers.

How do I connect router by using wireless?

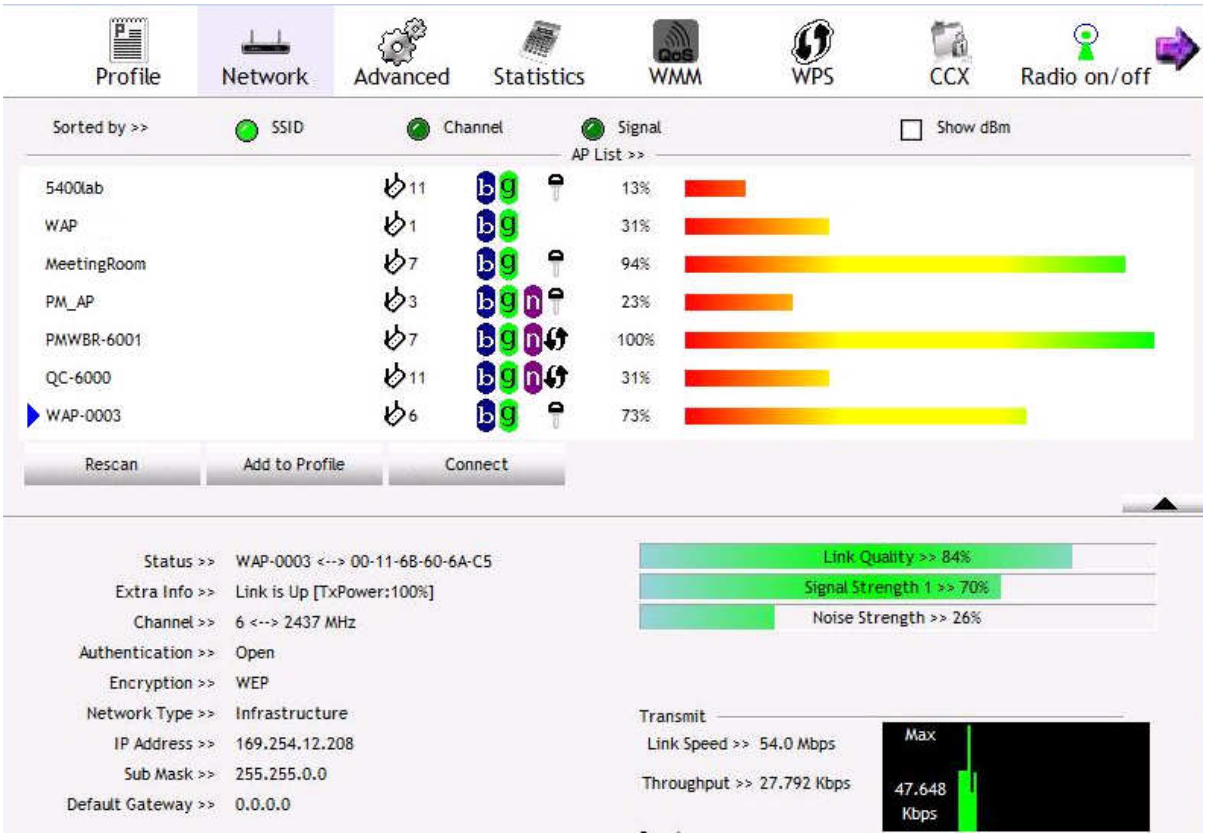
1. How to start to use wireless?

A: First, make sure that you already installed wireless client device in your computer. Then check the configuration of wireless router. The default is below:



About wireless client, you will see wireless icon:

Then click and will see the AP list that wireless client can be accessed:



If the client cannot find your wireless router, please refresh network list again.
Choose the one that you will want to connect and connect:

If successfully, the computer will show something similar.

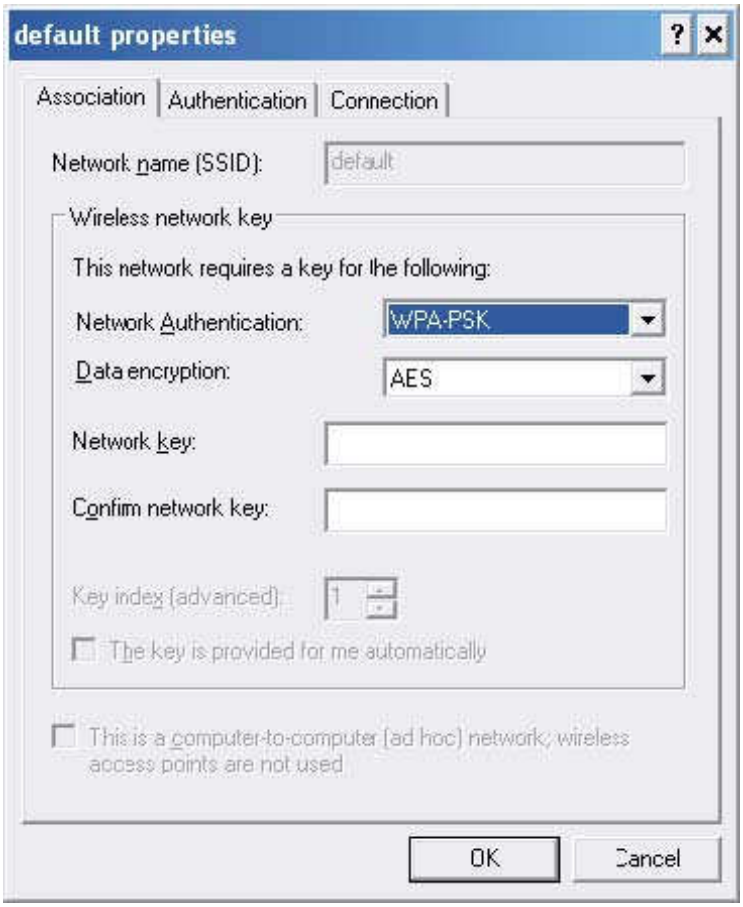
User will also retrieve IP from router, for example:

```
Connection-specific DNS Suffix  . :
IP Address. . . . . . . . . . . . : 192.168.1.123
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```

2. How can I use AES encryption of WPA-PSK to connect?

A: First, you must check if the driver of wireless client supports AES encryption. Please refer to the below:

If SSID is default and click “Properties” to check if the driver of wireless client supports AES encryption.



3. When I use wireless to connect the router, but I find the signal is very low even if I am close to the router?

A: Please check if the wireless client is normal, first. If yes, please send the unit to the seller and verify what the problem is.

Technical Specifications

General	
Model	WBR-6603 *150Mbps Wireless ADSL2+ Modem Router*
Data Transfer Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps Max physical rate up to 150 Mbps in 802.11n mode
Transmit Power	802.11b: 17±2dBm 802.11g: 14±2dBm 802.11n: 14±2dBm
Frequency Range	America/ FCC: 2.412~2.462GHz (11 Channels) Europe/ ETSI: 2.412~2.472GHz (13 Channels)
Modulation Schemes	DBPSK/DQPSK/CCK/OFDM
Channels	1~11 channels (FCC), 1~13 channels (ETSI),
Security	64/128-bits WEP Encryption, WPA-PSK, WPA2-PSK, WPA, WPA2, 802.1x
Diagnostic LED	Status ADSL WLAN LAN LEDs
Antenna	2dBi Dipole fix antenna
Physical and Environmental	
Operating Systems Supported	Windows 2000, Windows XP, Windows Vista, Windows 7, Linux, MAC OSX
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	10% ~ 90% RH, no condensation
Dimensions	150mm (L) x 110mm(W) x 28mm (D)
Certifications	FCC, CE, Wifi Certificate